

ADJOINT ORBITS OF MATRIX GROUPS OVER FINITE QUOTIENTS OF COMPACT DISCRETE VALUATION RINGS AND REPRESENTATION ZETA FUNCTIONS

MICHELE ZORDAN

ABSTRACT. This paper gives methods to describe the adjoint orbits of $\mathbf{G}(\mathfrak{o}_r)$ on $\mathrm{Lie}(\mathbf{G})(\mathfrak{o}_r)$ where $\mathfrak{o}_r = \mathfrak{o}/\mathfrak{p}^r$ ($r \in \mathbb{N}$) is a finite quotient of the localization \mathfrak{o} of the ring of integers of a number field at a prime ideal \mathfrak{p} and \mathbf{G} is a closed \mathbb{Z} -subgroup scheme of GL_n for an $n \in \mathbb{N}$. The main result is a classification of the adjoint orbits in $\mathrm{Lie}(\mathbf{G})(\mathfrak{o}_{r+1})$ whose reduction mod \mathfrak{p}^r contains $a \in \mathrm{Lie}(\mathbf{G})(\mathfrak{o}_r)$ in terms of the reduction mod \mathfrak{p} of the stabilizer of a for the $\mathbf{G}(\mathfrak{o}_r)$ -adjoint action. As an application, this result is then used to compute the representation zeta function of the principal congruence subgroups of $\mathrm{SL}_3(\mathfrak{o})$.

1. INTRODUCTION

1.1. Main results. Let \mathbf{G} be a smooth closed \mathbb{Z} -subgroup scheme of GL_n for some $n \in \mathbb{N}$. Let k be a number field with ring of integers \mathcal{O} . Let $\mathfrak{p} \triangleleft \mathcal{O}$ be a non-zero prime ideal such that the reduction mod \mathfrak{p}^r $\mathbf{G}(\mathfrak{o}) \rightarrow \mathbf{G}(\mathfrak{o}/\mathfrak{p}^r)$ is surjective for all $r \in \mathbb{N}$. By Hensel's lemma this happens for all but finitely many prime ideals of \mathcal{O} (see [24, Chapter II, Proposition 4.1]). Let π be a uniformizer for \mathfrak{p} and identify the residue field $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}$ with \mathbb{F}_q . For convenience of notation we shall set $\mathfrak{o} = \mathcal{O}_{\mathfrak{p}}$ and $\mathfrak{o}_r = \mathfrak{o}/\mathfrak{p}^r$.

DEFINITION 1.1. Let $r \in \mathbb{N}$ and $a \in \mathrm{Lie}(\mathbf{G})(\mathfrak{o}_r)$. We define the (*group*) *shadow*

$$\mathrm{Sh}_{\mathbf{G}(\mathfrak{o}_r)}(a) \leq \mathbf{G}(\mathbb{F}_q)$$

of a to be the reduction mod \mathfrak{p} of the group stabilizer of a for the adjoint action of $\mathbf{G}(\mathfrak{o}_r)$ on $\mathrm{Lie}(\mathbf{G})(\mathfrak{o}_r)$. Analogously, the *Lie shadow*

$$\mathrm{Sh}_{\mathrm{Lie}(\mathbf{G})(\mathfrak{o}_r)}(a) \leq \mathrm{Lie}(\mathbf{G})(\mathbb{F}_q)$$

of a is the reduction mod \mathfrak{p} of the centralizer of a in $\mathrm{Lie}(\mathbf{G})(\mathfrak{o}_r)$.

REMARK 1.2. Definition 1.1 borrows from [4, Definition 2.2]. The crucial difference here is that [4, Definition 2.2] also associates a conjugacy class of such shadows to each adjoint orbit in $\mathrm{Lie}(\mathbf{G})(\mathfrak{o}_r)$. Instead we shall work with single elements or we shall consider isomorphism types of shadows, thus obtaining a coarser invariant than the one described in [4].

ASSUMPTION 1.3. For the rest of the section we fix $r \in \mathbb{N}$ and $a \in \mathrm{Lie}(\mathbf{G})(\mathfrak{o}_r)$ having a lift to $\mathrm{Lie}(\mathbf{G})(\mathfrak{o}_{r+1})$ with the same shadow. We assume further that $\mathrm{Lie}(\mathbf{G})(\mathfrak{o})$ admits a non-degenerate invariant symmetric form.

The first main result concerns adjoint orbits in $\mathrm{Lie}(\mathbf{G})(\mathfrak{o}_r)$.

THEOREM A. *The set of $\mathbf{G}(\mathfrak{o}_{r+1})$ -adjoint orbits in $\mathrm{Lie}(\mathbf{G})(\mathfrak{o}_{r+1})$ containing a lift of the element a is in one to one correspondence with the set of orbits for the co-adjoint action of $\mathrm{Sh}_{\mathbf{G}(\mathfrak{o}_r)}(a)$ on*

$$\mathrm{Hom}_{\mathbb{F}_q}(\mathrm{Sh}_{\mathrm{Lie}(\mathbf{G})(\mathfrak{o}_r)}(a), \mathbb{F}_q).$$

In case $\mathbf{G} = \mathrm{GL}_n$, $\mathrm{Lie}(\mathbf{G})(\mathfrak{o})$ is equipped with the form $\mathrm{tr}(XY)$ and $r = 2$, Theorem A is [22, Theorem 1]. Indeed, as proved in [22, Lemma 6] for any $n \times n$ matrix over \mathbb{F}_q there is an $n \times n$ matrix over \mathfrak{o}_2 with the same shadow lifting it. With the further hypothesis of the existence of a lift with the same shadow (c.f. Assumption 1.3), the proof of Theorem A generalizes the strategies adopted by S. Jambor and W. Plesken in [22].

The second main result describes the shadow of a lift:

THEOREM B. *Let $x \in \mathrm{Lie}(\mathbf{G})(\mathfrak{o}_{r+1})$ be a lift of $a \in \mathrm{Lie}(\mathbf{G})(\mathfrak{o}_r)$, and let the orbit of x for the action of $\mathbf{G}(\mathfrak{o}_{r+1})$ be represented by the orbit of*

$$c \in \mathrm{Hom}_{\mathbb{F}_q}(\mathrm{Sh}_{\mathrm{Lie}(\mathbf{G})(\mathfrak{o}_r)}(a), \mathbb{F}_q)$$

in the one to one correspondence of Theorem A. Then

$$\mathrm{Sh}_{\mathbf{G}(\mathfrak{o}_{r+1})}(x) \cong \mathrm{Stab}_{\mathrm{Sh}_{\mathbf{G}(\mathfrak{o}_r)}(a)}(c),$$

where $\mathrm{Stab}_{\mathrm{Sh}_{\mathbf{G}(\mathfrak{o}_r)}(a)}(c)$ is the stabilizer of c for the dual of the $\mathrm{Sh}_{\mathbf{G}(\mathfrak{o}_r)}(a)$ -adjoint action on $\mathrm{Sh}_{\mathrm{Lie}(\mathbf{G})(\mathfrak{o}_r)}(a)$.

The third main result is a quantitative statement on the number of lifts of a matrix. Let $d = \dim_{\mathbb{F}_q} \mathrm{Lie}(\mathbf{G})(\mathbb{F}_q)$.

THEOREM C. *Let $S = \mathrm{Sh}_{G_r}(a)$ and T be the shadow of a lift of a to $\mathrm{Lie}(\mathbf{G})(\mathfrak{o}_{r+1})$. Let $\mathfrak{s} = \mathrm{Sh}_{\mathrm{Lie}(\mathbf{G})(\mathfrak{o}_r)}(a)$ and*

$$\lambda = |\{c \in \mathrm{Hom}_{\mathbb{F}_q}(\mathfrak{s}, \mathbb{F}_q) \mid \mathrm{Stab}_S(c) \cong T\}|,$$

where $\mathrm{Stab}_S(c)$ is defined as in Theorem B. Then the number of lifts of a with shadow isomorphic to T is equal to

$$q^{d - \dim_{\mathbb{F}_q} \mathfrak{s}} \lambda.$$

The fourth main result concerns representation zeta functions. Let $G = \mathbf{G}(\mathfrak{o})$ have finite abelianization (FAB for short) i.e. $|G/[G, G]| < \infty$. By [3, Proposition 2.1], G is (representation) rigid i.e. the number $r_i(G)$ of continuous complex i -dimensional irreducible representations is finite for each $i \in \mathbb{N}$, its *representation zeta function* is the Dirichlet series

$$\zeta_G(s) = \sum_{i=1}^{\infty} r_i(G) i^{-s},$$

where s is a complex variable. Theorems A and B are used to obtain the following result.

THEOREM D. *Let \mathfrak{o} be a compact discrete valuation ring of characteristic 0 whose residue field has cardinality $q > 2$ and characteristic $p \neq 3$. Then for all $m \in \mathbb{N}$ such that the m -principal congruence subgroup $\mathrm{SL}_3^m(\mathfrak{o})$ (c.f. Section 2.2.2 for a definition) is potent and saturable (c.f. [3, Section 2.1]),*

$$\zeta_{\mathrm{SL}_3^m(\mathfrak{o})}(s) = q^{8m} \frac{1 + u(q)q^{-3-2s} + u(q^{-1})q^{-2-3s} + q^{-5-5s}}{(1 - q^{1-2s})(1 - q^{2-3s})}$$

where $u(X) = X^3 + X^2 - X - 1 - X^{-1}$.

Notice that this result already appeared as part of [3, Theorem E] and was obtained again in [4] by different methods. Our proof of Theorem D resembles closely the one in [4], however we classify only the conjugacy classes of $\mathfrak{sl}_3(\mathfrak{o}/\mathfrak{p}^\ell)$ ($\ell \in \mathbb{N}$) having non-minimal dimensional centralizer and we do it according to the isomorphism type of their shadow rather than according to the conjugacy class of their shadow. Our approach moreover rests on two concepts: the presence of a shadow-preserving lift for all elements of $\mathrm{SL}_3(\mathfrak{o}/\mathfrak{p}^\ell)$ and all levels $\ell \in \mathbb{N}$ (a property that we call shadow-hereditariness) and Theorem C to quantitatively control the adjoint

orbit of traceless matrices over $\mathfrak{o}/\mathfrak{p}^\ell$ lifting a traceless matrix over $\mathfrak{o}/\mathfrak{p}^{\ell+1}$. These two facts, thanks to the most prominent role given to the shadow, simplify the computations appearing in [4] for what concerns principal congruence subgroups of $\mathrm{SL}_3(\mathfrak{o})$. Shadow-hereditariness does not hold in general for traceless matrices, indeed there are traceless 4×4 matrices over $\mathbb{Z}/p^3\mathbb{Z}$ that have no lift with the same shadow (see [34, Section 5.5.2]). This compromises the amenability of $\mathrm{SL}_n(\mathfrak{o})$ to the proposed method as it stands for $n \geq 4$. However, [34, Chapter 4] explains how this obstacle may be overcome by reducing the computation to matrices over the finite field and how Theorems A and B may still be exploited to compute the representation zeta function of the principal congruence subgroups of $\mathrm{SL}_4(\mathfrak{o})$ for odd residue field characteristic.

1.2. Background and motivation. In order to contextualize the main results of this paper and provide motivation for them, we now make a brief digression summarizing some known results on similarity classes.

When considering matrices over a field, the similarity classes are characterized by *rational* (or *Frobenius*) *canonical forms* (see D. Dummit and R. Foote [14, Section 12.2] for an introduction to this classical subject). However, when the base ring is not a field, even over \mathbb{Z} or its finite quotients, there is no such an elegant and concise theory. Nonetheless, over the years, many notable results have been proved. In [8] R. Davis showed that, for a rational prime p and $\ell \in \mathbb{N}$, two matrices in $\mathrm{Mat}_n(\mathbb{Z}/p^\ell\mathbb{Z})$, which are zeroes of a common polynomial whose reduction modulo p has no repeated roots, are similar if and only if they are similar modulo p . In a similar flavour and generalizing a result of D. Suprunenko [33], J. Pomfret showed that, over finite local rings, invertible $n \times n$ matrices with n coprime to the residue field characteristic are similar if and only if their reductions modulo p are similar (see [29]).

Another source of insights comes from the solution of the conjugacy problem for arithmetic groups achieved by F. Grunewald and D. Segal. In [17] F. Grunewald gave a method to determine if two matrices in $\mathrm{GL}_n(\mathbb{Q})$ are conjugate by an invertible matrix over \mathbb{Z} . The same author and D. Segal, described in [18] a more general algorithm to decide whether two elements of an arithmetic group are conjugate. For traceless 3×3 matrices over \mathbb{Z} , H. Appelgate and H. Onishi gave in [1] an independent solution to the problem, giving a more effective algorithm to determine whether two matrices of $\mathrm{SL}_3(\mathbb{Z})$ are similar. In [2], the same authors provided an elegant method to decide similarity of traceless matrices over \mathbb{Z}_p : two matrices in $\mathrm{SL}_n(\mathbb{Z}_p)$ are similar if and only if their reductions modulo p^ℓ are similar for all $\ell \in \mathbb{N}$. In particular, given $a, a' \in \mathrm{SL}_n(\mathbb{Z}_p)$ they find $\ell = \ell(a, a') \in \mathbb{N}$ and prove that if a and a' are conjugate in $\mathrm{SL}_n(\mathbb{Z}/p^\ell\mathbb{Z})$, then a and a' are conjugate in $\mathrm{SL}_n(\mathbb{Z}_p)$. This effectively reduces the conjugacy problem in the uncountable group $\mathrm{SL}_n(\mathbb{Z}_p)$ to a finite one.

For 3×3 matrices over $\mathbb{Z}/p^\ell\mathbb{Z}$ ($\ell \in \mathbb{N}$) – and slightly more generally over a finite quotient of a discrete valuation ring A modulo a power of its maximal ideal I – the first attempts of classifying the conjugacy classes date back at least to A. Nechaev [26], where the author described the similarity classes in $\mathrm{Mat}_3(\mathbb{Z}/p^2\mathbb{Z})$. A. Pizarro in [28] gave a complete classification for matrices over finite quotients of discrete valuation rings. More recently, in [5] N. Avni, U. Onn, A. Prasad and L. Vaserstein have extended the classification of A. Nechaev classifying similarity classes of 3×3 matrices over all finite quotients of A . This classification is explicit enough to allow them to enumerate the similarity classes in $\mathrm{Mat}_3(A/I^\ell)$ and the conjugacy classes of $\mathrm{GL}_3(A/I^\ell)$ for $\ell \in \mathbb{N}$ (see [5, Theorem 5.2]).

Even for $\ell = 2$, the conjugacy problem for matrices in $\mathrm{Mat}_{4n}(\mathbb{Z}/p^2\mathbb{Z})$ contains, according to S. Nagornyĭ [25, Section 4], the matrix pair similarity problem, which,

according to Ju. Drozd [12], is wild for general n . Nonetheless recent striking results have been obtained for similarity classes of matrices of arbitrary size over a local principal ideal ring of length 2. Let R be such a ring and let \mathbb{F}_q be its residue field. First, if R' is another local principal ideal ring of length 2, P. Singla [31] has shown that there is a canonical bijection between irreducible representations of $\mathrm{GL}_n(R)$ and of $\mathrm{GL}_n(R')$. In particular the number of conjugacy classes of these two groups is equal and only depends on the characteristic of the residue field. Second, S. Jambor and W. Plesken have proved that the similarity classes in $\mathrm{Mat}_n(R)$ whose image over the residue field \mathbb{F}_q is the similarity class of $a \in \mathrm{Mat}_n(\mathbb{F}_q)$ are in one to one correspondence with the orbits of group centralizer $C_{\mathrm{GL}_n(\mathbb{F}_q)}(a)$ acting on the \mathbb{F}_q -linear dual of the commuting algebra $C_{\mathrm{Mat}_n(\mathbb{F}_q)}(a)$. More recently, A. Prasad, P. Singla and S. Spallone have formulated and proved an equivalent result phrased in terms of the Ext functor (see [30, Remark 1.1 and Theorem 2.8]). Using this theory, they describe the similarity classes in $\mathrm{Mat}_n(R)$ for $n \leq 4$, together with their centralizers. This allows them to enumerate the similarity classes and the cardinalities of their centralizers as polynomials in q . In particular they show that the polynomials representing the number of similarity classes in $\mathrm{Mat}_n(R)$ have non-negative integer coefficients.

1.2.1. Zeta functions. When $R = A/I^2$, the computations in [30] give the number of similarity classes of $\mathrm{Mat}_n(R/I^\ell)$ for $\ell = 2$. If ℓ is allowed to vary, natural questions on properties of the number of similarity classes of $\mathrm{Mat}_n(R/I^\ell)$ as ℓ tends to infinity arise. Slightly more generally, for an A -group scheme $\mathbf{\Gamma}$, one studies the asymptotic behaviour of the number of $\mathbf{\Gamma}(A/I^\ell)$ -adjoint orbits on the associated Lie lattice $\mathrm{Lie}(\mathbf{\Gamma})(A/I^\ell)$. Such questions may be addressed by means of the *similarity class zeta function*

$$\zeta_{\mathrm{Lie}(\mathbf{\Gamma})(A)}^{\mathrm{sc}}(s) = \sum_{i \in \mathbb{N}} a_i^{\mathrm{sc}}(\mathrm{Lie}(\mathbf{\Gamma})(A)) q^{-is},$$

where $a_i^{\mathrm{sc}}(\mathrm{Lie}(\mathbf{\Gamma})(A))$ denotes the number of $\mathbf{\Gamma}(A/I^i)$ -adjoint orbits in $\mathrm{Lie}(\mathbf{\Gamma})(A/I^i)$ and s is a complex variable. Analytic properties of the similarity class zeta function correspond to arithmetic properties of the sequence $\mathcal{S}^{\mathrm{sc}} = \{a_i^{\mathrm{sc}}(\mathrm{Lie}(\mathbf{\Gamma})(A))\}_{i \in \mathbb{N}}$. For instance if $\zeta_{\mathrm{Lie}(\mathbf{\Gamma})(A)}^{\mathrm{sc}}$ is a rational function in q^{-s} then the numbers in $\mathcal{S}^{\mathrm{sc}}$ obey a linear recurrence relation or if $\zeta_{\mathrm{Lie}(\mathbf{\Gamma})(A)}^{\mathrm{sc}}$ has finite abscissa of convergence then the partial sums

$$\sum_{i \leq N} a_i^{\mathrm{sc}}(\mathrm{Lie}(\mathbf{\Gamma})(A))$$

grow polynomially with $N \in \mathbb{N}$. For odd residue field characteristic, N. Avni, U. Onn, A. Prasad and L. Vaserstein have computed $\zeta_{\mathfrak{gl}_3(A)}^{\mathrm{sc}}$ (cf. [5, Theorem 5.2]) while N. Avni, B. Klopsch, U. Onn, and C. Voll in [4, Theorem E] computed the similarity class zeta function of $\mathfrak{gu}_3(A)$. Both similarity class zeta functions are rational in q^{-s} and have abscissa of convergence 3.

One natural variation of the counting problem described above is to study the sequence of numbers of conjugacy classes of congruence quotients of $\mathbf{\Gamma}(A)$. More in detail, let $\mathbf{\Gamma}$ have an embedding into GL_n for some $n \in \mathbb{N}$. Its m -th principal congruence subgroups is the kernel of the reduction modulo I^m , i.e.

$$\mathbf{\Gamma}^m(A) = \ker(\mathbf{\Gamma}(A) \rightarrow \mathrm{GL}_n(A/I^m)).$$

The finite group $\mathbf{\Gamma}(A)/\mathbf{\Gamma}^m(A)$ has only a finite number of conjugacy classes that we denote with $a_m^{\mathrm{cc}}(\mathbf{\Gamma}(A))$. The associated Dirichlet generating function is known as the *conjugacy class zeta function* of $\mathbf{\Gamma}(A)$:

$$\zeta_{\mathbf{\Gamma}(A)}^{\mathrm{cc}}(s) = \sum_{i \in \mathbb{N}} a_i^{\mathrm{cc}}(\mathbf{\Gamma}(A)) q^{-is} \quad s \in \mathbb{C}.$$

Using model theoretic results of J. Denef and L. van den Dries in [10], M. du Sautoy [13] proves that if A is the ring of p -adic integers and $\Gamma(\mathbb{Z}_p)$ is a compact p -adic analytic group, then the conjugacy class zeta function is rational in q^{-s} . In particular this holds for $\Gamma = \mathrm{GL}_n$, establishing that there is a linear recurrence relation among the numbers of conjugacy classes of the groups $\mathrm{GL}_n(\mathbb{Z}/p^\ell\mathbb{Z})$ for $\ell \in \mathbb{N}$. More recently, extending the work of J. Pas [27], M. Berman, J. Derakhshan, U. Onn and P. Pajunen prove the same rationality result when Γ is a Chevalley group and the characteristic of A is arbitrary. In addition they establish that, fixed Γ , the conjugacy class zeta function only depends on the size of residue field of A (see [6, Theorem C]). This echoes in a more general setting the above mentioned uniformity result for $\ell = 2$ featuring in [31].

Another interesting application of classifying adjoint orbits in $\mathrm{Lie}(\Gamma)(\mathfrak{o})$ is the study of complex representations of $\Gamma(\mathfrak{o})$. We may arrange continuous complex representations of $\Gamma(\mathfrak{o})$ by their degree; the asymptotic properties of the sequence resulting from this counting problem are captured by the representation zeta function. Classes of groups whose representation zeta function has been studied so far comprise arithmetic groups and their principal congruence subgroups. For what concerns principal congruence subgroups of special linear groups, the Kirillov orbit method – when applicable – is a powerful linearization technique that relates irreducible representations and similarity classes. In [4] N. Avni, B. Klopsch, U. Onn and C. Voll use the classification of adjoint orbits in $\mathfrak{gl}_3(\mathfrak{o})$ and $\mathfrak{gu}_3(\mathfrak{o})$ to compute the representation zeta function of principal congruence subgroups of $\mathrm{SL}_3(\mathfrak{o})$ and $\mathrm{SU}_3(\mathfrak{o})$ in the same hypotheses of Theorem D.

1.3. Organization of the paper. We start off in Section 2 with a quick introduction to the vocabulary of group schemes over \mathbb{Z} , contextualizing this topic to the main purpose of the paper. We introduce a Lie theory for group schemes and the exponential map for closed subgroup schemes of GL_n . We conclude the section with a comparison between this Lie theory and the p -adic Lie theory for p -saturable principal congruence subgroups of $\mathbf{G}(\mathfrak{o})$; this is needed for the application of the results of Section 3 to the computation of representation zeta functions. All results contained in this section are well known to the experts but difficult to find in the literature from a unique source; we therefore, for the sake of completeness, included them with proofs. Section 3 introduces our version of the similarity class invariant called the *shadow*. We use it to generalize results of S. Jambor and W. Plesken (see [22]) and obtain Theorems A and B, from which Theorem C is then deduced. The section ends with a refinement of Theorem C for special linear groups that is more suited to be used in the computations of the following section.

Section 4 is devoted to applying the results in Section 3 to the computation of representation zeta functions. The section begins with a short summary of the main techniques that allow us build a bridge between the area of representation zeta functions and the topics in the previous section. These techniques include the Kirillov orbit method and the Poincaré series of a matrix of linear forms. The section then focuses on particularly interesting examples of Lie rings for which results in Section 3 hold, namely $\mathfrak{sl}_n(\mathfrak{o})$ for $n \in \mathbb{N}$. Provided it admits a shadow-preserving lift, we manage to quantitatively classify the lifts of a traceless matrix over a finite quotient of \mathfrak{o} according to the isomorphism type of its shadow. As a proof of concept, we apply this result by computing the representation zeta function of almost all principal congruence subgroups of $\mathrm{SL}_3(\mathfrak{o})$ for $q > 2$ and $3 \nmid q$, thus obtaining again the formula in [3, Theorem E].

1.4. Notation. We denote with \mathbb{N} the set of the positive integers $\{1, 2, \dots\}$, while $\mathbb{N}_0 = \{0, 1, 2, \dots\}$ are the natural numbers. Analogously, for $n \in \mathbb{N}$ we set $[n] =$

$\{1, \dots, n\}$ and $[n]_0 = \{0, \dots, n\}$. In this work, p is a rational prime. The field of p -adic numbers is denoted by \mathbb{Q}_p and the ring of p -adic integers by \mathbb{Z}_p . More generally, we denote with k a number field with ring of integers \mathcal{O} . Fixed a non-zero prime ideal $\mathfrak{p} \triangleleft \mathcal{O}$ we set $\mathfrak{o} = \mathcal{O}_{\mathfrak{p}}$ and denote by q the cardinality of the residue field $\mathbb{F}_q = \mathcal{O}/\mathfrak{p}$. The field of fractions of \mathfrak{o} is denoted with \mathfrak{k} and ν denotes the \mathfrak{p} -adic valuation both on \mathfrak{o} and \mathfrak{k} .

As conventional, the multiplicative group of a field \mathbf{K} is \mathbf{K}^* . We extend this notation to non-trivial \mathfrak{o} -modules as follows. Given such a module M , we write, for a given \mathfrak{p} , $M^* = M \setminus \mathfrak{p}M$. For the trivial \mathfrak{o} -module we set $\{0\}^* = \{0\}$. The Pontryagin dual of a compact abelian group \mathfrak{a} is

$$\widehat{\mathfrak{a}} = \text{Irr}(\mathfrak{a}) = \text{Hom}_{\mathbb{Z}}^{\text{cont}}(\mathfrak{a}, \mathbb{C}^*).$$

By analogy, we write $\widehat{G} = \text{Irr}(G)$ for the collection of continuous, irreducible complex characters of a profinite group G .

If R is a ring we write $R[[T]]$ for the ring of formal power series in T . For $m \in \mathbb{N}$ and $f \in R[[T]]$, $f \bmod T^m$ denotes the class of f in the quotient ring $R[[T]]/T^m$.

1.5. Acknowledgements. I am indebted to Christopher Voll and Benjamin Martin for their precious advice. I also wish to thank Tobias Rossmann, Giovanna Carnovale, Andrea Lucchini, Uri Onn and Alexander Stasinski for the interesting conversations and insightful comments on this work.

This work is part of my PhD thesis. I acknowledge financial support from the School of Mathematics of the University of Southampton, the Faculty of Mathematics of the University of Bielefeld and CRC 701.

2. GROUP SCHEMES AND p -ADIC LIE THEORY

2.1. Preliminaries on group schemes. An *affine scheme* X over \mathbb{Z} is a representable functor from the category of rings **Rng** to the category of sets **Set**. By this we mean that there is a ring $\mathcal{O}[X]$ such that X is naturally isomorphic to the functor $\text{Hom}_{\mathbb{Z}}(\mathcal{O}[X], -)$. A \mathbb{Z} -group functor is a functor from **Rng** to the category of groups **Grp**, an (*affine*) *group scheme* \mathbf{G} over \mathbb{Z} (or \mathbb{Z} -group scheme) is a \mathbb{Z} -group functor that is representable when considered as a functor from **Rng** to **Set**. A subfunctor of a \mathbb{Z} -group functor is called a *\mathbb{Z} -subgroup functor* and in similar fashion a \mathbb{Z} -subgroup functor of a \mathbb{Z} -group scheme which is also a subscheme is called a *\mathbb{Z} -subgroup scheme*. If A is a ring, we write $\text{Sp}A$ for the functor represented by the ring A ; *closed subschemes* of $\text{Sp}A$ are then subfunctors of the form $V(I)$ defined by

$$V(I)(R) = \{\varphi \in \text{Hom}_{\mathbb{Z}}(A, R) \mid \varphi(I) = 0\}$$

where I is an ideal of A (c.f. [9, I, §2, 6.2]).

Let \mathbf{G} be an affine group scheme over \mathbb{Z} , and let $\varphi : R \rightarrow S$ be a ring homomorphism. The functor \mathbf{G} associates with φ a group homomorphism $\mathbf{G}(\varphi) : \mathbf{G}(R) \rightarrow \mathbf{G}(S)$. Often, when it is clear from the context we shall, for convenience of notation, drop the \mathbf{G} from this notation and denote $\mathbf{G}(\varphi)$ with φ too. If R is a ring and $\rho \in \mathbf{G}(R)$, we write $\rho^{\#}$ for the morphism of functors sending $\psi \in \text{Sp}R(S)$ onto $\mathbf{G}(\psi)(\rho) \in \mathbf{G}(S)$.

2.1.1. The Lie algebra of a group functor. Let \mathbf{G} be a \mathbb{Z} -group functor and let R be a ring, if $R[T]$ is the algebra of polynomials in T with coefficients in R , we write ε for the class of $T \bmod T^2$ and $R(\varepsilon)$ for the quotient algebra $R[T]/T^2$. We have a decomposition $R(\varepsilon) = R \oplus \varepsilon R$ and homomorphisms $i : R \rightarrow R(\varepsilon)$, $\text{proj} : R(\varepsilon) \rightarrow R$ defined by $i(1) = 1$ and $\text{proj}(1) = 1$, $\text{proj}(\varepsilon) = 0$, such that $\text{proj} \circ i = \text{id}_R$.

Let \mathbf{G} be a group scheme over \mathbb{Z} . The homomorphisms i and proj define homomorphisms $\mathbf{G}(i)$ and $\mathbf{G}(\text{proj})$. The \mathbb{Z} -group functor $\text{Lie}(\mathbf{G})$ is defined by

$$\text{Lie}(\mathbf{G})(R) = \ker(\mathbf{G}(\text{proj})).$$

When no risk of confusion exists, by abuse of notation, $\mathbf{G}(i)$ and $\mathbf{G}(\text{proj})$ will also be indicated with i and proj . Let \mathbf{H} be another \mathbb{Z} -group functor and let $f : \mathbf{G} \rightarrow \mathbf{H}$ be a homomorphism (i.e. a natural transformation such that for each ring S , $f(S) : \mathbf{G}(S) \rightarrow \mathbf{H}(S)$ is a group homomorphism). The group homomorphism $f(R(\varepsilon))$ induces a group homomorphism

$$\text{Lie}(\mathbf{G})(f) : \text{Lie}(\mathbf{G})(R) \rightarrow \text{Lie}(\mathbf{H})(R)$$

sending each $x \in \text{Lie}(\mathbf{G})(R)$ to $\text{Lie}(f)(R)(x) = f(R(\varepsilon))(i(x))$. For convenience of notation, in applying $\text{Lie}(f)(R)$ to $x \in \text{Lie}(\mathbf{G})(R)$, we write $\text{Lie}(f)(x)$ instead of $\text{Lie}(f)(R)(x)$.

2.1.2. The exponential notation. It is customary to write the group law of $\text{Lie}(\mathbf{G})$ additively; we inherit the following notation from [9]. If S is an R -algebra and α is an element of S of vanishing square, then there is a unique R -algebra homomorphism $R(\varepsilon) \rightarrow S$ sending ε onto α . The image of $x \in \text{Lie}(\mathbf{G})(R)$ under the composite homomorphism

$$\text{Lie}(\mathbf{G})(R) \rightarrow \mathbf{G}(R(\varepsilon)) \rightarrow \mathbf{G}(S)$$

will be written $e^{\alpha x}$. In particular, in $R(\varepsilon)$, $x = e^{\varepsilon x}$. For $x, y \in \text{Lie}(\mathbf{G})(R)$ we thus have in $\mathbf{G}(S)$

$$e^{\alpha(x+y)} = e^{\alpha x} e^{\alpha y}.$$

2.1.3. The adjoint action. The group $\mathbf{G}(R)$ acts on $\text{Lie}(\mathbf{G})(R)$ in the following way: let g be an element of $\mathbf{G}(R)$ and $x \in \text{Lie}(\mathbf{G})(R)$, we set

$$\text{Ad}_g(x) = i(g) x i(g)^{-1}.$$

If we write $\text{GL}(\text{Lie}(\mathbf{G}))$ for the \mathbb{Z} -group functor of linear automorphisms of $\text{Lie}(\mathbf{G})$ we may define a homomorphism

$$\text{Ad} : \mathbf{G} \rightarrow \text{GL}(\text{Lie}(\mathbf{G}))$$

which we call the adjoint action of \mathbf{G} . This in turn defines a homomorphism

$$\text{ad} = \text{Lie}(\text{Ad}) : \text{Lie}(\mathbf{G}) \rightarrow \text{Lie}(\text{GL}(\text{Lie}(\mathbf{G})))$$

by means of which one defines $[x, y] = \text{ad}(x)(y)$ for all $x, y \in \text{Lie}(\mathbf{G})(R)$. This gives $\text{Lie}(\mathbf{G})(R)$ the structure of an R -Lie ring. For convenience of notation, we shall write

$$\text{ad}_x = \text{ad}(x) : \text{Lie}(\mathbf{G})(R) \rightarrow \text{Lie}(\mathbf{G})(R).$$

2.1.4. The linear group. We now introduce a very important example of \mathbb{Z} -group scheme, namely the (general) linear group. If V is a \mathbb{Z} -module (i.e. an abelian group) and R is a ring, $\mathcal{L}(V \otimes_{\mathbb{Z}} R)$ denotes the monoid of all endomorphisms of the R -module $V \otimes_{\mathbb{Z}} R$. We define a \mathbb{Z} -monoid functor $\text{End}(V)$ by setting

$$\text{End}(V)(S) = \mathcal{L}(V \otimes_{\mathbb{Z}} S) \quad (S \in \mathbf{Rng}).$$

[9, II, §, 2.4] shows that $\text{End}(V)$ is an affine scheme over \mathbb{Z} when V is finitely generated and projective over \mathbb{Z} (i.e. V is a free finitely generated abelian group). The *linear group* of V , denoted by $\text{GL}(V)$, is the largest subgroup functor of $\text{End}(V)$. By loc. cit. and references therein, if V is free and finitely generated, then $\text{GL}(V)$ is an affine group scheme over \mathbb{Z} . In particular, when $V = \mathbb{Z}^n$, we write

$$\text{GL}_n = \text{GL}(V).$$

Let $n \in \mathbb{N}$ and take $\mathbf{G} = \mathrm{GL}_n$. By [9, II, §4, 4.12] and references therein, $\mathrm{Lie}(\mathbf{G})(R)$ may be identified with the Lie ring $\mathrm{End}(\mathbb{Z}^n)(R)$, with $e^{\varepsilon x} = \mathrm{id} + \varepsilon x$, the adjoint representation being given by

$$\mathrm{Ad}_g(x) = g \circ x \circ g^{-1} \quad (g \in \mathrm{GL}_n(R), x \in \mathrm{End}(\mathbb{Z}^n)(R)).$$

and the Lie bracket being the Lie commutator.

If \mathbf{H} is a subgroup scheme of \mathbf{G} , $\mathrm{Lie}(\mathbf{H})(R)$ may be identified with the Lie subring of $\mathrm{End}(\mathbb{Z}^n)(R)$ consisting of elements for which $\mathrm{id} + \varepsilon x$ is contained in $\mathbf{H}(R(\varepsilon))$.

2.2. Exponential map. The goal of this section is to establish a parallel between the Lie theory for group schemes and p -adic Lie theory. This will be done by comparing the p -adic \exp and \log maps with the exponential map for group schemes. The following proposition introduces the exponential map in characteristic 0 and is inspired by [9, II, §6, 3.1]. We borrow from there the following convention: given a linearly topologized and complete R -algebra S , and a topologically nilpotent element t of S , we write $f(t)$ for the element of $\mathbf{G}(S)$ which is the image of $f(T) \in \mathbf{G}(R[[T]])$ under the continuous morphism of $R[[T]]$ into S sending T onto t . Therefore for instance, we shall have $f(\varepsilon)$ of $\mathbf{G}(R(\varepsilon))$ and the element $f(T + T')$ of $\mathbf{G}(R[[T, T']])$.

PROPOSITION 2.1. *Let R be a ring with $\mathrm{char} R = 0$ and let \mathbf{G} be an affine group scheme over \mathbb{Z} . Then for each $x \in \mathrm{Lie}(\mathbf{G})(R)$ there is a unique element $\exp(Tx)$ of $\mathbf{G}(R[[T]])$ such that*

- a. $\exp(\varepsilon x) = e^{\varepsilon x}$ in $\mathbf{G}(R(\varepsilon))$,
- b. $\exp((T + T')x) = \exp(Tx) \exp(T'x)$ in $\mathbf{G}(R[[T, T']])$.

PROOF. Fix $x \in \mathrm{Lie}(\mathbf{G})(R)$. Let $\varepsilon_1, \dots, \varepsilon_m$ be m variables of vanishing square and let $R_m = R(\varepsilon_1, \dots, \varepsilon_m) = R_{m-1}(\varepsilon_m)$. Consider the element X_m of $\mathbf{G}(R_m)$ defined by

$$X_m = e^{\varepsilon_1 x} \dots e^{\varepsilon_m x}.$$

By [9, II, §4, 4.2],

$$e^{\varepsilon_i x} e^{\varepsilon_j x} = e^{\varepsilon_i \varepsilon_j [x, x]} e^{\varepsilon_j x} e^{\varepsilon_i x} = e^{\varepsilon_j x} e^{\varepsilon_i x}$$

for all $i, j \in \{1, \dots, m\}$, so the element X_m is invariant under permutations of the variables ε_i 's.

Let $a_m : R[[T]]/T^{n+1} \rightarrow R_m$ be the R -homomorphism defined by $a_m(T) = \varepsilon_1 + \dots + \varepsilon_m$. Since $\mathrm{char} R = 0$, a_m is a bijection onto the subring $R_n^{S_m}$ consisting of the invariants of R_m under the permutations of ε_i 's. We now show that there is a unique element E_m of $\mathbf{G}(R[[T]]/T^{m+1})$ such that $a_m(E_m) = X_m$. Indeed, \mathbf{G} is affine i.e. $\mathbf{G}(R_m)$ is naturally isomorphic to $\mathrm{Hom}_{\mathbb{Z}}(\mathcal{O}[\mathbf{G}], R_m)$. It follows that the invariants for the S_m -action on $\mathbf{G}(R_m)$ induced by the S_m -action on R_m are

$$\mathbf{G}(R_n)^{S_m} = \mathrm{Hom}_{\mathbb{Z}}(\mathcal{O}[\mathbf{G}], R_m)^{S_m} = \mathrm{Hom}_{\mathbb{Z}}(\mathcal{O}[\mathbf{G}], R_n^{S_m}) = \mathbf{G}(R_n^{S_m}).$$

Hence X_m belongs to $\mathbf{G}(\mathrm{im} a_m)$ and therefore is of the form $a_m(E_m)$, where

$$E_m \in \mathbf{G}(R[[T]]/T^{m+1}).$$

By passing to the limit $m \rightarrow \infty$ we now construct $E \in \mathbf{G}(R[[T]])$ such that

$$E_m = E(T \bmod T^{m+1})$$

for each m . In order to prove that such an element exists, consider the following commutative diagram

$$\begin{array}{ccc} R[T]/T^{m+1} & \xrightarrow{a_m} & R_m \\ \downarrow p_m & & \downarrow q_m \\ R[T]/T^m & \xrightarrow{a_{m-1}} & R_{m-1}, \end{array}$$

where p_m is the canonical map and q_m sends ε_i onto ε_i for $i \neq m$ and annihilates ε_m . The commutativity of the previous diagram, implies that, being each E_m a homomorphism $\mathcal{O}[\mathbf{G}] \rightarrow R[T]/T^{m+1}$, the collection of all E_m ($m \in \mathbb{N}$) is an inverse limit system; so there is a homomorphism $\mathcal{O}[\mathbf{G}] \rightarrow R[[T]]$ associated with an element $E(T)$ of $\mathbf{G}(R[[T]])$. To prove uniqueness, let $E'(T)$ be another element of $\mathbf{G}(R[[T]])$ such that

$$(2.1) \quad E_m = E'(T \bmod T^{m+1})$$

for each $m \in \mathbb{N}$. Let $\ker(E(T)^\#, E'(T)^\#)$ be the scheme that to each ring S assigns

$$\ker(E(T)^\#(S), E'(T)^\#(S)) = \{x \in \mathrm{Sp}(R[[T]])(S) \mid E(T)^\#(x) = E'(T)^\#(x)\}.$$

Since \mathbf{G} is affine it is separated (see [23, I 2.6 (10)]). Hence, by [9, I §2, 7.6], $\ker(E(T)^\#, E'(T)^\#)$ is closed in $\mathrm{Sp}(R[[T]])$ and is defined by an ideal of I of $R[[T]]$. By (2.1), we have $I \subseteq T^{m+1}R[[T]]$ for each m , so that $I = 0$ and $E(T) = E'(T)$.

The proof that E meets conditions a. and b. and is unique is, mutatis mutandis, the same as the proof of the corresponding parts of [9, II, §6, 3.1]. \square

2.2.1. Closed subgroups of the linear group. We shall now focus on a particular type of group schemes: closed subgroup schemes of the linear group. From this point onwards \mathbf{G} denotes a smooth closed \mathbb{Z} -subgroup scheme of GL_n ($n \in \mathbb{N}$). We also fix the following notation: k is a number field with ring of integers \mathcal{O} , $\mathfrak{p} \triangleleft \mathcal{O}$ is a non-zero prime ideal of \mathcal{O} with residue field characteristic p and π is a uniformizer for \mathfrak{p} . Moreover we denote $\mathcal{O}_{\mathfrak{p}}$ with \mathfrak{o} and, for $r \in \mathbb{N}$, we write $\mathfrak{o}_r = \mathfrak{o}/\mathfrak{p}^r$.

REMARK 2.2. For each $x \in \mathrm{Lie}(\mathbf{G})(\mathfrak{o})$,

$$\exp(Tx) = \sum_{i \geq 0} \frac{T^i x^i}{i!}.$$

On the right-hand side, x^i ($i \in \mathbb{N}$) denotes the i -fold matrix multiplication of x with itself. Notice, moreover, that [11, Lemma 6.20] ensures that it makes sense to define the formal power series in T on the right-hand side of the equality above.

PROOF. Fix $x \in \mathrm{Lie}(\mathbf{G})(\mathfrak{o})$. First of all we observe that, since \mathbf{G} is a closed subgroup scheme of GL_n , [9, II, §4, 4.2] shows that

$$e^{\varepsilon x} = \mathrm{id} + \varepsilon x.$$

Let $m \in \mathbb{N}$ and let $\varepsilon_1, \dots, \varepsilon_m, a_m, X_m, E_m$ be as in the proof of Proposition 2.1. Also, recall that, E_m is the unique element of $\mathbf{G}(\mathfrak{o}[T]/T^{m+1})$ such that

$$\begin{aligned} E_m &\equiv \exp(Tx) \pmod{T^{m+1}} \\ X_m &= a_m(E_m). \end{aligned}$$

It follows that

$$\begin{aligned} X_m &= (\mathrm{id} + \varepsilon_1 x) \cdots (\mathrm{id} + \varepsilon_m x) \\ &= \mathrm{id} + (\varepsilon_1 + \cdots + \varepsilon_m)x + \cdots + (\varepsilon_1 \cdots \varepsilon_m)x^m \\ &= \mathrm{id} + tx + \cdots + \left(\frac{t^m}{m!}\right)x^m \end{aligned}$$

where $t = a_m(T \bmod T^{m+1})$. By the uniqueness of E_m it follows that

$$E_m \equiv \sum_{i=0}^m \frac{T^i x^i}{i!} \bmod T^{m+1}.$$

As $\exp(Tx)$ is defined by taking the limit of the inverse system formed by the E_m 's, this concludes the proof. \square

REMARK 2.3. Let $r \in \mathbb{N}$. The exponential map $\exp : \mathrm{Lie}(\mathbf{G})(\mathfrak{o}) \rightarrow \mathbf{G}(\mathfrak{o}[[T]])$ induces an exponential map

$$\exp_r : \mathrm{Lie}(\mathbf{G})(\mathfrak{o}_r) \rightarrow \mathbf{G}(\mathfrak{o}_r[[T]]).$$

In other words, for each $x \in \mathrm{Lie}(\mathbf{G})(\mathfrak{o}_r)$ there is a unique element $\exp_r(Tx)$ such that

- a. $\exp_r(\varepsilon x) = e^{\varepsilon x}$ in $\mathbf{G}(\mathfrak{o}_r(\varepsilon))$,
- b. $\exp_r((T + T')x) = \exp_r(Tx) \exp_r(T'x)$ in $\mathbf{G}(\mathfrak{o}_r[[T, T']])$.

For convenience of notation, when there is no risk of confusion, we shall denote \exp_r with \exp as well. Following the same arguments contained in [9, II, §6, 3.4], the uniqueness statement in Remark 2.3 implies the following corollary.

COROLLARY 2.4. *Let $x \in \mathrm{Lie}(\mathbf{G})(\mathfrak{o}_r)$. Then in $\mathrm{GL}(\mathrm{Lie}(\mathbf{G})(\mathbb{Z}))(\mathfrak{o}_r[[T]])$ we have*

$$\mathrm{Ad}_{\exp(Tx)} = \sum_{i \geq 0} \frac{T^i \mathrm{ad}_x^i}{i!}.$$

When $x \in \pi \mathrm{Lie}(\mathbf{G})(\mathfrak{o}_r)$, then $\exp(Tx) \in \mathbf{G}(\mathfrak{o}_r[[T]])$ and we define $\exp(x)$ as the image of $\exp(Tx)$ under the homomorphism $\mathfrak{o}_r[[T]] \rightarrow \mathfrak{o}_r$ sending T to 1. In practice we may, then, replace T by 1 in Corollary 2.4 obtaining

$$(2.2) \quad \mathrm{Ad}_{\exp(x)} = \sum_{i \geq 0} \frac{\mathrm{ad}_x^i}{i!}.$$

PROPOSITION 2.5. *If $x \in \pi \mathfrak{gl}_n(\mathfrak{o}_r)$ then $x \in \pi \mathrm{Lie}(\mathbf{G})(\mathfrak{o}_r)$ if and only if $\exp(x) \in \mathbf{G}(\mathfrak{o}_r)$.*

PROOF. We start by observing that if $x \in \pi \mathrm{Lie}(\mathbf{G})(\mathfrak{o}_r)$, then $\exp(Tx) \in \mathbf{G}(\mathfrak{o}_r[[T]])$, so we may replace T with 1 obtaining $\exp(x) \in \mathbf{G}(\mathfrak{o}_r)$. Moreover, by taking the Weil restriction of \mathbf{G} (c.f. [7, Section A.5]) we may assume, within the proof of this statement, that $\mathfrak{o} = \mathbb{Z}_p$.

Let t be the valuation of the entry of x with the lowest valuation. We observe that, as $\mathbf{G}(\mathfrak{o}_r)$ is a group and $\exp(x) \in \mathbf{G}(\mathfrak{o}_r)$,

$$\exp(x)^{p^{r-t-1}} \in \mathbf{G}(\mathfrak{o}_r).$$

Now, $\mathfrak{o}_r \cong \mathbb{Z}/p^r\mathbb{Z}$ and therefore, for each $\bar{a} \in \mathfrak{o}_r$ and $a \in \mathbb{Z}$ such that $a \equiv \bar{a} \bmod p^r$, we have

$$\exp(x)^a = \exp(\bar{a}x).$$

This implies that $\exp(p^{r-t-1}x) = \mathrm{id} + p^{r-t-1}x \in \mathbf{G}(\mathfrak{o}_r)$, and this is equivalent to $p^{r-t-1}x \in \mathrm{Lie}(\mathbf{G})(\mathfrak{o}_r)$, which in turn is equivalent to $x \in \mathrm{Lie}(\mathbf{G})(\mathfrak{o}_r)$. \square

2.2.2. *Two Lie theories.* A p -saturable group G (c.f. [3, Section 2.1] for a definition) carries a Lie structure associated with it, namely $\mathrm{L}(G) = (G, +, [\cdot, \cdot])$ where

$$\begin{aligned} x + y &= \lim_{n \rightarrow \infty} (x^{p^n} y^{p^n})^{p^{-n}} \\ [x, y] &= \lim_{n \rightarrow \infty} [x^{p^n}, y^{p^n}]^{p^{-2n}} \end{aligned} \quad (\text{for } x, y \in G),$$

(c.f. [15, Section 4] for details).

We shall now consider some concrete examples of p -saturable subgroups of $\mathbf{G}(\mathfrak{o})$ and compare the construction above with $\mathrm{Lie}(\mathbf{G})(\mathfrak{o})$. Let $m \in \mathbb{N}$, recall that the m -th principal congruence subgroup of $\mathbf{G}(\mathfrak{o})$ is

$$\mathbf{G}^m(\mathfrak{o}) = \{g \in \mathbf{G}(\mathfrak{o}) \mid g \equiv \mathrm{id} \pmod{\mathfrak{p}^m}\}.$$

[3, Proposition 2.3] (when phrased for groups) ensures that $\mathbf{G}^m(\mathfrak{o})$ is p -saturable for almost all m : namely, when $m > e \cdot (p-1)^{-1}$, where $e = e(\mathfrak{o}, \mathbb{Z}_p)$ is the absolute ramification index of \mathfrak{o} .

PROPOSITION 2.6. *Let $m \in \mathbb{N}$ be such that $\mathbf{G}^m(\mathfrak{o})$ and $\mathrm{GL}_n^m(\mathfrak{o})$ are both saturable pro- p groups. Then $\mathrm{L}(\mathbf{G}^m(\mathfrak{o}))$ and $\pi^m \mathrm{Lie}(\mathbf{G})(\mathfrak{o})$ are isomorphic as Lie rings.*

PROOF. For reasons analogous to the ones adduced in the proof of Proposition 2.5, we may assume $\mathfrak{o} = \mathbb{Z}_p$ for the rest of the proof of this statement. The saturability of $\mathrm{GL}_n^m(\mathbb{Z}_p)$ implies that the exponential series

$$\mathcal{E}(x) = \sum_{i \geq 0} \frac{x^i}{i!}$$

converges in $\mathrm{GL}_n^m(\mathbb{Z}_p)$ for all $x \in \mathrm{Lie}(\mathbf{G})(\mathbb{Z}_p)$. It follows that we may replace T with 1 in the identity of Remark 2.2, obtaining $\mathcal{E}(x) \in \mathbf{G}^m(\mathbb{Z}_p)$. As \mathbf{G} is closed in GL_n , we have that $\mathbf{G}^m(\mathbb{Z}_p)$ is closed in $\mathrm{GL}_n^m(\mathbb{Z}_p)$ in the profinite topology, and since it is also saturable, $\mathrm{L}(\mathbf{G}^m(\mathbb{Z}_p))$ is a Lie sub-lattice of $\mathrm{L}(\mathrm{GL}_n^m(\mathbb{Z}_p))$.

Let now $x \in \pi^m \mathfrak{gl}_n(\mathbb{Z}_p)$ such that $\exp(x) \in \mathbf{G}^m(\mathbb{Z}_p)$, this implies that, for all $r \in \mathbb{N}$, $\exp(x)$ belongs to $\mathbf{G}^m(\mathbb{Z}/p^r\mathbb{Z}) \bmod p^r$; so by Proposition 2.5, x belongs to $p^m \mathrm{Lie}(\mathbf{G})(\mathbb{Z}/p^r\mathbb{Z})$ for all $r \in \mathbb{N}$. It follows that $x \in p^m \mathrm{Lie}(\mathbf{G})(\mathbb{Z}_p)$ if and only if $\exp(x) \in \mathbf{G}^m(\mathbb{Z}_p)$.

By [24, Proposition 8.2], \exp establishes an isomorphism between $p^m \mathfrak{gl}_n(\mathbb{Z}_p)$ and $\mathrm{L}(\mathrm{GL}_n^m(\mathbb{Z}_p))$, so its restriction to $p^m \mathrm{Lie}(\mathbf{G})(\mathbb{Z}_p)$ makes it isomorphic to $\mathrm{L}(\mathbf{G}^m(\mathbb{Z}_p))$. \square

3. ADJOINT ORBITS IN LIE RINGS

Let $\mathfrak{p} \triangleleft \mathcal{O}$ be a non-zero prime ideal such that the reduction mod \mathfrak{p}^r

$$\mathbf{G}(\mathcal{O}_{\mathfrak{p}}) \rightarrow \mathbf{G}(\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^r)$$

is surjective for all $r \in \mathbb{N}$.

Recall that $\mathfrak{o} = \mathcal{O}_{\mathfrak{p}}$, $\mathfrak{o}_r = \mathfrak{o}/\mathfrak{p}^r$, we denote $G = \mathbf{G}(\mathfrak{o})$ and $\mathfrak{g} = \mathrm{Lie}(\mathbf{G})(\mathfrak{o})$; analogously, for all $r \in \mathbb{N}$, $G_r = \mathbf{G}(\mathfrak{o}_r)$ and $\mathfrak{g}_r = \mathrm{Lie}(\mathbf{G})(\mathfrak{o}_r)$. For convenience of notation we write $\bar{G} = G_1 = \mathbf{G}(\mathbb{F}_q)$ and $\bar{\mathfrak{g}} = \mathfrak{g}_1 = \mathrm{Lie}(\mathbf{G})(\mathbb{F}_q)$.

Let $r, t \in \mathbb{N}$ be positive integers with $r < t$, we define $\theta_{t,r} : \mathfrak{o}_t \rightarrow \mathfrak{o}_r$ to be the reduction modulo \mathfrak{p}^r . For simplicity also the reduction modulo \mathfrak{p}^r on \mathfrak{g}_t will be called $\theta_{t,r}$. In the same spirit the reduction modulo \mathfrak{p}^r on \mathfrak{o} will be denoted with θ_r and the same symbol will also denote the reduction modulo \mathfrak{p}^r on \mathfrak{g} . The map $\theta_{t,r} : \mathfrak{o}_t \rightarrow \mathfrak{o}_r$ induces a map $G_t \rightarrow G_r$ that we shall call $\Theta_{t,r}$.

3.1. Shadows. Fix $r \in \mathbb{N}$ and $a \in \mathfrak{g}_{r+1}$. We denote the group and the Lie centralizer of a with

$$\begin{aligned} C_{G_r}(a) &= \{g \in G_r \mid gag^{-1} = a\} \\ C_{\mathfrak{g}_r}(a) &= \{x \in \mathfrak{g}_r \mid [x, a] = 0\} \end{aligned}$$

respectively.

REMARK 3.1. Recall from Definition 1.1 that the (group) shadow and the Lie shadow of a are respectively The (group) shadow is

$$\begin{aligned}\mathrm{Sh}_{G_r}(a) &= \Theta_{r,1}(\mathrm{C}_{G_r}(a)) \leq \bar{G} \\ \mathrm{Sh}_{\mathfrak{g}_r}(a) &= \theta_{r,1}(\mathrm{C}_{\mathfrak{g}_r}(a)) \leq \bar{\mathfrak{g}}.\end{aligned}$$

Notice that the $\mathrm{C}_{G_r}(a)$ -conjugation on $\mathrm{C}_{\mathfrak{g}_r}(a)$ induces a $\mathrm{Sh}_{G_r}(a)$ -action by conjugation on $\mathrm{Sh}_{\mathfrak{g}_r}(a)$.

If $b \in \theta_{r,r+1}^{-1}(a)$ and $\tilde{\mathcal{C}}$ denotes its G_{r+1} -orbit, then $\tilde{\mathcal{C}} \cap \theta_{r,r+1}^{-1}(a)$ is an orbit of the action of

$$\tilde{S} = \Theta_{r,r+1}^{-1}(\mathrm{C}_{G_r}(a))$$

on $\theta_{r,r+1}^{-1}(a)$. To see this, let $g \in G_{r+1}$ be such that $g.b \in \theta_{r,r+1}^{-1}(a)$, it follows that $\theta_{r,r+1}(g.b) = \Theta_{r,r+1}(g).a = a$, which implies $g \in \tilde{S}$.

3.2. Action of the first principal congruence subgroup. Let Υ be the restriction of $\Theta_{r+1,1}$ to \tilde{S} . Following the approach of [22], we proceed in two stages: first we consider the orbits for the action of the normal subgroup $\tilde{N} = \ker \Upsilon \trianglelefteq \tilde{S}$ and then we act on them with the factor group $\tilde{S}/\tilde{N} = \mathrm{Sh}_{G_r}(a)$. The following analogous to [22, Lemma 5] describes the \tilde{N} -orbits in $\theta_{r,r+1}^{-1}(a)$.

LEMMA 3.2. *Let $b \in \theta_{r,r+1}^{-1}(a)$, There is a one to one correspondence between $\pi^r \mathrm{coker} \pi \mathrm{ad}_b$ and the \tilde{N} -orbits in $\theta_{r,r+1}^{-1}(a)$.*

PROOF. We describe the \tilde{N} -conjugation in $\theta_{r,r+1}^{-1}(a)$ in terms of b and the image of ad_b . We start by writing elements of $\theta_{r,r+1}^{-1}(a)$ in terms of b . Indeed, the latter is a preimage of a for the map $\theta_{r,r+1}$. As any other preimage of a differs from b by an element that is 0 modulo \mathfrak{p}^r , it follows that

$$(3.1) \quad \theta_{r,r+1}^{-1}(a) = \{b + \pi^r z \mid z \in \mathfrak{g}_{r+1}\}.$$

By Proposition 2.5 an element of \tilde{N} is of the form $\exp(\pi y)$ for some $\pi y \in \pi \mathfrak{g}_{r+1}$. Now we are able to explicitly describe the \tilde{N} -conjugation in $\theta_{r,r+1}^{-1}(a)$. Fix $z \in \mathfrak{g}_{r+1}$ and $y \in \pi \mathfrak{g}_{r+1}$. Let also $x = b + \pi^r z \in \theta_{r,r+1}^{-1}(a)$ and $g = \exp(\pi y)$. Then

$$\begin{aligned}gxg^{-1} &= \mathrm{Ad}_{\exp(\pi y)}(x) \\ &= \sum_{i \geq 0} \frac{\mathrm{ad}_{\pi y}^i(x)}{i!} && \text{by (2.2)} \\ &= b + \pi^r z + \sum_{i \geq 1} \left(\frac{\mathrm{ad}_{\pi y}^i(b)}{i!} + \frac{\mathrm{ad}_{\pi y}^i(\pi^r z)}{i!} \right) \\ &= b + \pi^r z + \sum_{i \geq 1} \frac{\mathrm{ad}_{\pi y}^i(b)}{i!} && ([\pi y, \pi^r z] \equiv 0 \pmod{\mathfrak{p}^{r+1}}).\end{aligned}$$

We now show that $\mathrm{ad}_{\pi y}^i(b) \equiv 0 \pmod{\mathfrak{p}^{r+1}}$, for $i \geq 2$. To prove this, recall that $\exp(\pi y) \in \tilde{S} = \Theta_{r,r+1}^{-1}(\mathrm{C}_{G_r}(a))$, therefore

$$(3.2) \quad \mathrm{Ad}_{\exp(\pi y)}(b) \equiv \sum_{i \geq 0} \frac{\mathrm{ad}_{\pi y}^i(b)}{i!} \equiv b \pmod{\mathfrak{p}^r},$$

and this happens if and only if $\mathrm{ad}_{\pi y}(b) \equiv 0 \pmod{\mathfrak{p}^r}$. It follows that

$$(3.3) \quad gxg^{-1} = b + \pi^r z + \pi[y, b].$$

This shows that two lifts of a , say $b + \pi^r z$ and $b + \pi^r z'$ ($z, z' \in \mathfrak{g}_{r+1}$), are \tilde{N} -conjugate if and only if there exists $v \in \mathfrak{g}_{r+1}$ such that $\pi^r(z - z') = \pi[b, v]$. We conclude that the \tilde{N} -orbits in $\theta_{r,r+1}^{-1}(a)$ are in one to one correspondence with the elements of $\pi^r \text{coker } \pi \text{ad}_b$. \square

REMARK 3.3. Let $s, t \in \mathbb{N}$ with $s < t$ and let M be a left \mathfrak{o}_t -module, then $\pi^{t-s}M$ may be viewed as an \mathfrak{o}_s -module. Indeed, for all $\alpha \in \mathfrak{o}_s$ and $x \in M$, we define $\alpha x = \hat{\alpha}x$, where $\hat{\alpha} \in \mathfrak{o}_t$ is a lift of α . This definition is unambiguous for the left multiplication of elements of $\pi^{t-s}M$ by elements of \mathfrak{p}^s results in 0.

In view of the last remark, we can formulate and prove the following lemma.

LEMMA 3.4. *Let b be as in Lemma 3.2. Then $\pi^r \text{coker } \pi \text{ad}_b \cong \pi^{r-1} \text{coker } \text{ad}_a$ as \mathbb{F}_q -vector spaces.*

PROOF. Let

$$\begin{aligned} \Phi_r : \pi \mathfrak{gl}_n(\mathfrak{o}_{r+1}) &\longrightarrow \mathfrak{gl}_n(\mathfrak{o}_r) \\ \pi u &\longmapsto u', \end{aligned}$$

where u' is the reduction modulo \mathfrak{p}^r of u , and let φ_r be the restriction of Φ_r to $\pi \mathfrak{g}_{r+1}$. The map $\varphi_r : \pi \mathfrak{g}_{r+1} \rightarrow \mathfrak{g}_r$ defines an isomorphism of \mathfrak{o}_r -modules. As $\varphi_r(\text{im } \pi \text{ad}_b) = \text{im } \text{ad}_a$, we have that φ_r induces an isomorphism $\bar{\varphi}_r$ of \mathbb{F}_q -vector spaces between $\pi^r \text{coker } \pi \text{ad}_b$ and $\pi^{r-1} \text{coker } \text{ad}_a$. \square

NOTATION 3.5. For further usage, we fix the name φ_r for the restriction to $\pi \mathfrak{g}_{r+1}$ of the map Φ_r defined in the proof of Lemma 3.4 and we denote with $\bar{\varphi}_r$ the \mathbb{F}_q -linear isomorphism between $\pi^r \text{coker } \pi \text{ad}_b$ and $\pi^{r-1} \text{coker } \text{ad}_a$ induced by φ_r as explained in the proof of Lemma 3.4.

Lemma 3.4 allows us to substitute $\pi^r \text{coker } \pi \text{ad}_b$ with $\pi^{r-1} \text{coker } \text{ad}_a$ on which $\text{Sh}_{G_r}(a)$ acts with the action induced by the bijection $\bar{\varphi}_r$.

3.3. Action of the factor group. We shall now investigate the action of the factor group $\tilde{S}/\tilde{N} = \text{Sh}_{G_r}(a)$ on the set of orbits for the \tilde{N} -action on $\theta_{r,r+1}^{-1}(a)$; i.e. we shall describe the action of $\text{Sh}_{G_r}(a)$ on $\pi^{r-1} \text{coker } \text{ad}_a$.

DEFINITION 3.6. The centralizer $C_{G_r}(a)$ acts naturally by conjugation on $\pi^{r-1}A$. Since $\exp(\pi \mathfrak{g}_r) \cap C_{G_r}(a)$ is in its kernel, this action induces a $\text{Sh}_{G_r}(a)$ -action on $\pi^{r-1} \mathfrak{g}_r$; namely an element $c \in \text{Sh}_{G_r}(a)$ acts on $\pi^{r-1} \mathfrak{g}_r$ by conjugating by any of its lifts to $C_{G_r}(a)$. We call this the action of $\text{Sh}_{G_r}(a)$ on $\pi^{r-1} \mathfrak{g}_r$ by *conjugation by lifts* or $\text{Sh}_{G_r}(a)$ -conjugation by lifts. Explicitly, if $\bar{c} \in \text{Sh}_{G_r}(a)$ and $c \in C_{G_r}(a)$ is a lift of \bar{c} , for all $x \in \pi^{r-1} \mathfrak{g}_r$, we write

$$\bar{c}.x = cxc^{-1}.$$

The $\text{Sh}_{G_r}(a)$ -conjugation by lifts on $\pi^{r-1} \mathfrak{g}_r$ induces an action on $\pi^{r-1} \text{coker } \text{ad}_a$. Indeed, let $y \in \pi^{r-1} \mathfrak{g}_r$, $\bar{c} \in \text{Sh}_{G_r}(a)$ and let $c \in C_{G_r}(a)$ be a lift of \bar{c} . As c commutes with a

$$\bar{c}.[a, y] = c(ay - ya)c^{-1} = acyc^{-1} - cyac^{-1} = [a, \bar{c}.y].$$

This implies that, denoting with $\Gamma_{r,\bar{c}}$ the linear automorphism of $\pi^{r-1} \mathfrak{g}_r$ defined by $x \mapsto \bar{c}.x$, and with ρ_r the projection of $\pi^{r-1} \mathfrak{g}_r$ onto

$$\pi^{r-1}(\mathfrak{g}_r / \text{im } \text{ad}_a) = \pi^{r-1} \text{coker } \text{ad}_a,$$

there is a uniquely well defined \mathbb{F}_q -linear endomorphism $\bar{\Gamma}_{r,\bar{c}}$ of $\pi^{r-1} \text{coker ad}_a$ that makes the following diagram commute

$$\begin{array}{ccc} \pi^{r-1} \mathfrak{g}_r & \xrightarrow{\Gamma_{r,\bar{c}}} & \pi^{r-1} \mathfrak{g}_r \\ \rho_r \downarrow & & \downarrow \rho_r \\ \pi^{r-1} \text{coker ad}_a & \xrightarrow{\bar{\Gamma}_{r,\bar{c}}} & \pi^{r-1} \text{coker ad}_a. \end{array}$$

The rule $\bar{c} \mapsto \bar{\Gamma}_{r,\bar{c}}$ defines a $\text{Sh}_{G_r}(a)$ -action on $\pi^{r-1} \text{coker ad}_a$.

We shall now show that the $\text{Sh}_{G_r}(a)$ -action on $\pi^{r-1} \text{coker ad}_a$ induced by $\bar{\varphi}_r$ and resulting from the action of $\tilde{S}/\tilde{N} = \text{Sh}_{G_r}(a)$ on the set of orbits of the \tilde{N} -conjugation in $\theta_{r,r+1}^{-1}(a)$ is indeed the $\text{Sh}_{G_r}(a)$ -action on $\pi^{r-1} \text{coker ad}_a$ described above. Analogously to the approach of [22, Section 2.2], the key to do this is finding a lift b of a with the same shadow. What we mean is made precise in the following definitions:

DEFINITION 3.7. Let $r \in \mathbb{N}$. We say that $b \in \mathfrak{g}_{r+1}$ is *shadow-preserving lift* of a when $\theta_{r,r+1}(b) = a$ and $\text{Sh}_{G_{r+1}}(b) = \text{Sh}_{G_r}(a)$.

DEFINITION 3.8. We say that a group shadow S is *hereditary* if, for every $r \in \mathbb{N}$, every $x \in \mathfrak{g}_r$ such that $\text{Sh}_{G_r}(x) = S$ admits a shadow-preserving lift. If every shadow of \mathfrak{g}_t is hereditary for all $t \in \mathbb{N}$, we say that \mathfrak{g} is *shadow-hereditary*.

EXAMPLE 3.9. By [4, Lemma 6.4], the Lie ring $\mathfrak{sl}_3(\mathfrak{o})$ is shadow-hereditary.

The next lemma concludes this subsection.

LEMMA 3.10. Assume that the element a admits a shadow-preserving lift. Then the action of $\text{Sh}_{G_r}(a)$ on $\pi^{r-1} \text{coker ad}_a$ induced by $\bar{\varphi}_r$ is the linear action induced by the $\text{Sh}_{G_r}(a)$ -conjugation by lifts.

PROOF. Let $b \in \mathfrak{g}_{r+1}$ be a shadow-preserving lift of a . Analogously to Definition 3.6 the group $\text{Sh}_{G_{r+1}}(b)$ acts on $\pi^r \mathfrak{g}_{r+1}$ by conjugation by lifts; as b is shadow-preserving, this becomes an action of $\text{Sh}_{G_r}(a)$ and it induces a $\text{Sh}_{G_r}(a)$ -action on $\pi^r \text{coker } \pi \text{ad}_b$ in a way analogous to how $\text{Sh}_{G_r}(a)$ induces an action on $\pi^{r-1} \text{coker ad}_a$. Moreover these two actions commute with $\bar{\varphi}_r$; in other words, if $\bar{c} \in \text{Sh}_{G_r}(a)$, the action by \bar{c} on $\pi^r \mathfrak{g}_{r+1}$ defines \mathbb{F}_q -linear automorphisms $\Gamma_{r+1,\bar{c}}$ of $\pi^r \mathfrak{g}_{r+1}$ and all cells in the following diagram commute

$$(3.4) \quad \begin{array}{ccc} \pi^r \text{coker } \pi \text{ad}_b & \xrightarrow{\bar{\Gamma}_{r+1,\bar{c}}} & \pi^r \text{coker } \pi \text{ad}_b \\ \rho_{r+1} \uparrow & & \uparrow \rho_{r+1} \\ \pi^r \mathfrak{g}_{r+1} & \xrightarrow{\Gamma_{r+1,\bar{c}}} & \pi^r \mathfrak{g}_{r+1} \\ \varphi_r \downarrow & & \downarrow \varphi_r \\ \pi^{r-1} \mathfrak{g}_r & \xrightarrow{\Gamma_{r,\bar{c}}} & \pi^{r-1} \mathfrak{g}_r \\ \rho_r \downarrow & & \downarrow \rho_r \\ \pi^{r-1} \text{coker ad}_a & \xrightarrow{\bar{\Gamma}_{r,\bar{c}}} & \pi^{r-1} \text{coker ad}_a, \end{array}$$

where ρ_{r+1} is the projection of $\pi^r \mathfrak{g}_{r+1}$ onto $\pi^r \text{coker } \pi \text{ad}_b$ and $\bar{\Gamma}_{r+1,\bar{c}}$ is the \mathbb{F}_q -linear automorphism induced by $\Gamma_{r+1,\bar{c}}$.

It follows that it suffices to prove that the $\text{Sh}_{G_r}(a)$ -conjugation by lifts on $\pi^r \mathfrak{g}_{r+1}$ induces the $\text{Sh}_{G_r}(a)$ -action on $\pi^r \text{coker } \pi \text{ad}_b$ obtained by letting $\tilde{S}/\tilde{N} = \text{Sh}_{G_r}(a)$ act on the set of orbits of the \tilde{N} -conjugation in $\theta_{r,r+1}^{-1}(a)$. Let $c \in \text{Sh}_{G_r}(a)$. Since b has the same shadow as a , we can choose $\tilde{c} \in C_{G_{r+1}}(b)$ lifting c . In order to see how \tilde{c} acts on $\pi^r \text{coker } \pi \text{ad}_b$, first we see how it acts on an arbitrary lift of a :

$$\tilde{c}(b + \pi^r x) \tilde{c}^{-1} = b + \pi^r \tilde{c} x \tilde{c}^{-1}.$$

This last equation and Lemma 3.2 imply that the orbit of $\tilde{c}(b + \pi^r x) \tilde{c}^{-1}$ corresponds to the class of $\pi^r \tilde{c} x \tilde{c}^{-1}$ in $\pi^r \text{coker } \pi \text{ad}_b$. By (3.4), this allows us to conclude. \square

3.4. Intrinsic description of the orbits. So far we have established a one to one correspondence between the G_{r+1} -orbits in \mathfrak{g}_{r+1} intersecting $\theta_{r,r+1}^{-1}(a)$ non-trivially and $\text{Sh}_{G_r}(a)$ -conjugacy orbits in $\pi^{r-1} \text{coker } \text{ad}_a$. Now we replace $\pi^{r-1} \text{coker } \text{ad}_a$ with the more intrinsic dual of the Lie shadow.

NOTATION 3.11. Let $t \in \mathbb{N}$. Given an \mathfrak{o}_t -module M we write M^\sharp for its dual, i.e. $M^\sharp = \text{Hom}_{\mathfrak{o}_t}(M, \mathfrak{o}_t)$. Thus, for instance we write

$$\text{Sh}_{\mathfrak{g}_r}(a)^\sharp = \text{Hom}_{\mathbb{F}_q}(\text{Sh}_{\mathfrak{g}_r}(a), \mathbb{F}_q).$$

Let $C = \text{Sh}_{G_r}(a)$. The \mathfrak{o}_r -module $\pi^{r-1}(\ker \text{ad}_a)^\sharp = \pi^{r-1} \text{Hom}_{\mathfrak{o}_r}(\ker \text{ad}_a, \mathfrak{o}_r)$ becomes a $\mathbb{F}_q C$ -module in a natural way by considering the dual action of the C -conjugation by lifts on $\pi^{r-1} \mathfrak{g}_r$. Moreover

$$\pi^{r-1} \text{Hom}_{\mathfrak{o}_r}(\ker \text{ad}_a, \mathfrak{o}_r) \cong \text{Hom}_{\mathfrak{o}_r}(\pi^{r-1} \ker \text{ad}_a, \pi^{r-1} \mathfrak{o}_r)$$

as $\mathbb{F}_q C$ -modules via the isomorphism

$$\pi^{r-1} \alpha \mapsto \alpha|_{\pi^{r-1} \ker \text{ad}_a}.$$

By Remark 3.3

$$\text{Hom}_{\mathfrak{o}_r}(\pi^{r-1} \ker \text{ad}_a, \pi^{r-1} \mathfrak{o}_r) \cong \text{Hom}_{\mathbb{F}_q}(\theta_{r,1}(\ker \text{ad}_a), \mathbb{F}_q) = \text{Sh}_{\mathfrak{g}_r}(a)^\sharp,$$

hence it suffices to see that $\pi^{r-1} \text{coker } \text{ad}_a$ and $\pi^{r-1}(\ker \text{ad}_a)^\sharp$ are isomorphic as $\mathbb{F}_q C$ -modules.

ASSUMPTION 3.12. From now onwards we assume that \mathfrak{g} admits a non-degenerate symmetric invariant bilinear form.

EXAMPLE 3.13. The assumption above might seem rather obscure at first. However Cartan's criterion for semisimplicity (see for instance [20, Section III.4]) ensures that when \mathbf{G} is semisimple, $\text{Lie}(\mathbf{G})(\mathbb{C})$ admits such a form, namely the Killing form. Excluding finitely many primes, this remains valid for $\text{Lie}(\mathbf{G})(\mathfrak{o})$.

LEMMA 3.14. *The $\mathbb{F}_q C$ -modules $\pi^{r-1} \text{coker } \text{ad}_a$ and $\pi^{r-1}(\ker \text{ad}_a)^\sharp$ are isomorphic.*

PROOF. Consider the dual map of ad_a , i.e. the map $\text{ad}_a^\sharp : \mathfrak{g}_r^\sharp \rightarrow \mathfrak{g}_r$ defined by $f \mapsto f \circ \text{ad}_a$. Along the same lines of the proof of [22, Lemma 8], we first prove that $\pi^{r-1} \text{coker } \text{ad}_a$ and $\pi^{r-1}(\ker \text{ad}_a^\sharp)^\sharp$ are isomorphic as $\mathbb{F}_q C$ -modules. The evaluation

$$\begin{aligned} \alpha_1 : \text{coker } \text{ad}_a &\longrightarrow (\ker \text{ad}_a^\sharp)^\sharp \\ x + \text{im } \text{ad}_a &\longmapsto (\psi \mapsto \psi(x)) \end{aligned}$$

is an isomorphism of \mathfrak{o}_r -modules and it induces an isomorphism of \mathbb{F}_q -vector spaces

$$\bar{\alpha}_1 : \pi^{r-1} \text{coker } \text{ad}_a \rightarrow \pi^{r-1}(\ker \text{ad}_a^\sharp)^\sharp.$$

Moreover $\pi^{r-1}(\ker \operatorname{ad}_a^\#)^\#$ is a $\mathbb{F}_q C$ -module in a natural way by the dual of the C -conjugation and one checks that, when $\pi^{r-1}(\ker \operatorname{ad}_a^\#)^\#$ is equipped with this $\mathbb{F}_q C$ -module structure, $\bar{\alpha}_1$ becomes an $\mathbb{F}_q C$ -module homomorphism.

The second step consists in proving that $\pi^{r-1} \ker \operatorname{ad}_a \cong \pi^{r-1} \ker \operatorname{ad}_a^\#$ as $\mathbb{F}_q C$ -modules. Indeed κ induces a non-degenerate invariant \mathfrak{o}_r -bilinear form κ_r on \mathfrak{g}_r . This in turn establishes an \mathfrak{o}_r -modules isomorphism

$$\begin{aligned} \alpha_2 : \ker \operatorname{ad}_a &\longrightarrow \ker \operatorname{ad}_a^\# \\ x &\longmapsto (y \mapsto \kappa_r(y, x)), \end{aligned}$$

and, since κ_r is invariant, α_2 induces an $\mathbb{F}_q C$ -modules isomorphism

$$\bar{\alpha}_2 : \pi^{r-1} \ker \operatorname{ad}_a \rightarrow \pi^{r-1} \ker \operatorname{ad}_a^\#.$$

□

REMARK 3.15. Under the identification of $\pi^{r-1} \mathfrak{g}_r$ with $\bar{\mathfrak{g}}$, $\pi^r \ker \operatorname{ad}_a$ corresponds to $\operatorname{Sh}_{\bar{\mathfrak{g}}}(a)$. Indeed the identification is given by the isomorphism $\varphi : \pi^{r-1} \mathfrak{g}_r \rightarrow \bar{\mathfrak{g}}$ defined by $\pi^{r-1} x \mapsto \theta_{r,1}(x)$. It thus suffices to prove that

$$\operatorname{im} \varphi|_{\pi^{r-1} \ker \operatorname{ad}_a} = \operatorname{Sh}_{\bar{\mathfrak{g}}}(a).$$

Let $x \in C_{\mathfrak{g}_r}(a)$, and $\bar{x} = \theta_{r,1}(x) \in \operatorname{Sh}_{\bar{\mathfrak{g}}}(a)$. By definition, $\pi^{r-1} x \in \ker \operatorname{ad}_a$. Thus $\varphi(\pi^{r-1} x) = \bar{x}$ and we conclude.

Let $\bar{\alpha}_1$ and $\bar{\alpha}_2$ be as in the proof of Lemma 3.14. For further usage and convenience of notation we define

$$\begin{aligned} (3.5) \quad \gamma = \bar{\alpha}_2^\# \circ \bar{\alpha}_1 : \pi^{r-1} \operatorname{coker} \operatorname{ad}_a &\longrightarrow \operatorname{Sh}_{\bar{\mathfrak{g}}}(a)^\# \\ \pi^{r-1} x + \operatorname{im} \operatorname{ad}_a &\longmapsto (y \mapsto \kappa_1(\theta_{r,1}(x), y)). \end{aligned}$$

3.4.1. *Proof of Theorem A.* If a admits a shadow-preserving lift, then Lemmata 3.2, 3.4 and 3.14, imply that the \tilde{N} -orbits of elements lying above a correspond to the elements of $\operatorname{Sh}_{\bar{\mathfrak{g}}}(a)^\#$. By Lemmata 3.10 and 3.14, the \tilde{S}/\tilde{N} -action on the set of \tilde{N} -orbits $\operatorname{Sh}_{\bar{\mathfrak{g}}}(a)^\#$ is the dual of the $\operatorname{Sh}_{G_r}(a)$ -conjugation on $\operatorname{Sh}_{\bar{\mathfrak{g}}}(a)$. This proves Theorem A.

THEOREM A. *Assume that \mathfrak{g} admits a non-degenerate invariant symmetric form and that $a \in \mathfrak{g}_r$ has a shadow-preserving lift in the sense of Definition 3.7. Then the set of G_{r+1} -orbits in \mathfrak{g}_{r+1} for the action by conjugation intersecting $\theta_{r,r+1}^{-1}(a)$ non-trivially is in one to one correspondence with the set of $\operatorname{Sh}_{G_r}(a)$ -orbits in $\operatorname{Sh}_{\bar{\mathfrak{g}}}(a)^\#$.*

3.5. **Centralizer and shadow of a lift.** Given $a \in \mathfrak{g}_r$ and a similarity class $\tilde{C} \subseteq \mathfrak{g}_{r+1}$ lying above a , we shall now describe $\operatorname{Sh}_{G_{r+1}}(x)$ and $\operatorname{Sh}_{\bar{\mathfrak{g}}_{r+1}}(x)$ for $x \in \tilde{C}$.

THEOREM B. *Assume that \mathfrak{g} admits a non-degenerate invariant symmetric form and that $a \in \mathfrak{g}_r$ admits a shadow-preserving lift. Let $x \in \mathfrak{g}_{r+1}$ be a lift of $a \in \mathfrak{g}_r$, and let the orbit of x for the action of G_{r+1} be represented by the orbit of $c \in \operatorname{Sh}_{\bar{\mathfrak{g}}}(a)^\#$ in the one to one correspondence of Theorem A. Then*

$$\operatorname{Sh}_{G_{r+1}}(x) \cong \operatorname{Stab}_{\operatorname{Sh}_{G_r}(a)}(c).$$

PROOF. Choose $b \in \theta_{r,r+1}^{-1}(a)$ with the same shadow as a and write

$$x = b + \pi^r x_c.$$

Replacing c with an other element in its same $\text{Sh}_{G_r}(a)$ -orbit if necessary, we may assume that

$$(3.6) \quad \gamma(\varphi_r(\pi^r x_c + \text{im } \pi \text{ad}_b)) = c.$$

Now let $h \in \Theta_{r+1,1}^{-1}(\text{Sh}_{G_r}(a))$. As the restriction of the reduction modulo \mathfrak{p} to $C_{G_{r+1}}(b)$ is surjective onto $\text{Sh}_{G_r}(a)$, there is $h' \in C_{G_{r+1}}(b)$ such that $h \equiv h' \pmod{\mathfrak{p}^r}$, i.e. $h = h' \exp(\pi y)$ for some $y \in \mathfrak{g}_{r+1}$. As a result, h acts on x as follows

$$\begin{aligned} h(b + \pi^r x_c) h^{-1} &= h' \exp(\pi y) (b + \pi^r x_c) \exp(-\pi y) h'^{-1} \\ &= h' (b + \pi^r x_c + \pi[y, b]) h'^{-1} \\ &= b + h' (\pi^r x_c + \pi[y, b]) h'^{-1} \end{aligned}$$

It follows that h stabilizes x if and only if h' stabilizes $\pi^r x_c + \text{im } \pi \text{ad}_b$ in π^r coker πad_b and, by (3.6), this is equivalent to $\Theta_{r+1,1}(h') = \Theta_{r+1,1}(h)$ stabilizing c . \square

REMARK 3.16. In the notation of Theorem B, let H be the kernel of the reduction mod \mathfrak{p} from $C_{G_{r+1}}(x)$ to $\text{Sh}_{G_{r+1}}(x)$. Then H is isomorphic to the additive group of $C_{\mathfrak{g}_r}(a)$.

PROOF. As in the proof of Theorem B, let us write

$$x = b + \pi^r x_c.$$

Let $z \in \mathfrak{g}_{r+1}$. By (2.2) and the proof of Lemma 3.2, an element of the form $\exp(\pi z)$ acts as follows:

$$\text{Ad}_{\exp(\pi^r z)}(b + \pi^r x_c) = b + \pi^r x_c + \pi[z, b].$$

Hence $\exp(\pi z)$ fixes x if and only if $\pi z \in C_{\mathfrak{g}_{r+1}}(b)$. It follows that H is isomorphic to the additive group of $C_{\mathfrak{g}_r}(a)$ via φ_r . \square

3.6. Number of lifts. We are now in position to prove Theorem C.

THEOREM C. *Assume that $\text{Lie}(\mathbf{G})(\mathfrak{o})$ admits a non-degenerate invariant symmetric form and that $a \in \text{Lie}(\mathbf{G})(\mathfrak{o}_r)$ admits a shadow-preserving lift. Let $S = \text{Sh}_{G_r}(a)$ and T be the shadow of a lift of a to $\text{Lie}(\mathbf{G})(\mathfrak{o}_{r+1})$. Let $\mathfrak{s} = \text{Sh}_{\text{Lie}(\mathbf{G})(\mathfrak{o}_r)}(a)$ and*

$$\lambda = |\{c \in \text{Hom}_{\mathbb{F}_q}(\mathfrak{s}, \mathbb{F}_q) \mid \text{Stab}_S(c) \cong T\}|,$$

where $\text{Stab}_S(c)$ is defined as in Theorem B. Then the number of lifts of a with shadow isomorphic to T is equal to

$$q^{\dim_{\mathbb{F}_q} \text{Lie}(\mathbf{G})(\mathbb{F}_q) - \dim_{\mathbb{F}_q} \mathfrak{s}} \lambda.$$

PROOF. Let e be the number of lifts of a with shadow isomorphic to T and f be the number of orbits lying above a whose elements have shadow isomorphic to T . First we show that the cardinality of such orbits only depends on a and T . Let $b \in \mathfrak{g}_{r+1}$ be a lift of a with $\text{Sh}_{G_{r+1}}(b) \cong T$ and let $\hat{\mathcal{C}}$ be its G_{r+1} -adjoint orbit. By the orbit-stabilizer theorem and Remark 3.16,

$$|\hat{\mathcal{C}}| = \frac{|G_{r+1}|}{|\text{Sh}_{G_{r+1}}(b)| |C_{\mathfrak{g}_r}(a)|}.$$

So the cardinality of $\hat{\mathcal{C}}$ does not depend on the choice of b .

Let \mathcal{C} be the G_r -adjoint orbit of a . All the fibres of the restriction of $\theta_{r,r+1}$ to $\hat{\mathcal{C}}$ have the same cardinality, thus

$$|\hat{\mathcal{C}}|/|\mathcal{C}|$$

is the number of lifts of a in each G_{r+1} -orbit whose elements have shadow isomorphic to b and that intersects $\theta_{r,r+1}^{-1}(a)$ non-trivially. It follows that

$$e = \frac{|\hat{\mathcal{C}}|}{|\mathcal{C}|} f.$$

Let us expand $|\hat{\mathcal{C}}|/|\mathcal{C}|$: by the orbit-stabilizer theorem, this is equal to

$$\frac{|G_{r+1}|}{|G_r|} \frac{|C_{G_r}(a)|}{|C_{G_{r+1}}(b)|}$$

and by Remark 3.16,

$$\begin{aligned} |C_{G_r}(a)| &= |\text{Sh}_{G_r}(a)| \cdot |\pi \mathfrak{g}_r \cap C_{\mathfrak{g}_r}(a)| \\ |C_{G_{r+1}}(b)| &= |\text{Sh}_{G_{r+1}}(b)| \cdot |C_{\mathfrak{g}_r}(a)|; \end{aligned}$$

so

$$|\hat{\mathcal{C}}|/|\mathcal{C}| = \frac{|\text{Sh}_{G_r}(a)|}{|\text{Sh}_{G_{r+1}}(b)|} \frac{|\pi \mathfrak{g}_r \cap C_{\mathfrak{g}_r}(a)|}{|C_{\mathfrak{g}_r}(a)|}.$$

Since $|C_{\mathfrak{g}_r}(a)| = |\text{Sh}_{\mathfrak{g}_r}(a)| \cdot |\pi \mathfrak{g}_r \cap C_{\mathfrak{g}_r}(a)|$, we immediately see that

$$\frac{|\pi \mathfrak{g}_r \cap C_{\mathfrak{g}_r}(a)|}{|C_{\mathfrak{g}_r}(a)|} = |\text{Sh}_{\mathfrak{g}_r}(a)|^{-1}.$$

The quantity $|\text{Sh}_{G_r}(a)|/|\text{Sh}_{G_{r+1}}(b)|$ is, by Theorem B, the size of the $\text{Sh}_{G_r}(a)$ -orbit in $\text{Sh}_{\mathfrak{g}_{r+1}}(a)^\sharp$ corresponding to $\hat{\mathcal{C}}$ by Theorem A. Therefore, by definition,

$$\frac{|\text{Sh}_{G_r}(a)|}{|\text{Sh}_{G_{r+1}}(b)|} f = \lambda.$$

By Lemma 3.19 and Definition 3.21, $|\text{Sh}_{\mathfrak{g}_r}(a)| = q^{\dim_{\mathbb{F}_q} \mathfrak{s}}$, while $\frac{|G_{r+1}|}{|G_r|} = q^{\dim_{\mathbb{F}_q} \mathfrak{g}}$ and we conclude. \square

3.7. Special linear groups. When the group scheme in question is a special linear group, Theorem C may be refined for handier application. Recall that \mathfrak{o} is the localization of a ring of integers \mathcal{O} in a number field at a prime ideal \mathfrak{p} . Assume that \mathfrak{o} is such that $\mathfrak{sl}_n(\mathfrak{o})$ admits a non-degenerate invariant bilinear form.

REMARK 3.17. The normalized Killing form of [3, Section 5] is non-degenerate on $\mathfrak{sl}_n(\mathfrak{o})$ for almost all prime ideals $\mathfrak{p} \triangleleft \mathcal{O}$.

Let $\mathbf{H} = \text{SL}_n$, analogously to the notation used so far we define $\mathfrak{h} = \mathfrak{sl}_n(\mathfrak{o})$, $\bar{\mathfrak{h}} = \mathfrak{sl}_n(\mathbb{F}_q)$ and, for $t \in \mathbb{N}$, $\mathfrak{h}_t = \mathfrak{sl}_n(\mathfrak{o}_t)$. Let also $d = n^2 - 1$. [4, Lemma 2.3] tells us that, for special linear groups, the group shadow determines the Lie shadow; we need the following definition in order to precisely state this fact.

DEFINITION 3.18. Let $r \in \mathbb{N}$. Given a group-shadow S , we define

$$\text{As}(S) = \text{Span}(S) \cap \bar{\mathfrak{h}},$$

where $\text{Span}(S)$ is the additive span of S when considered as a subset of $\text{Mat}_n(\mathbb{F}_q)$.

Let $a \in \mathfrak{h}_r$ with $\text{Sh}_{G_r}(a) = S$. The following shows that $\text{Sh}_{\mathfrak{h}_r}(a)$ only depends on S and not directly on a .

LEMMA 3.19 ([4, Lemma 2.3]). Assume $q > 2$. Let $a \in \mathfrak{h}_r$ with $\text{Sh}_{G_r}(a) = S$, then $\text{Sh}_{\mathfrak{h}_r}(a) = \text{As}(S)$.

The next step is to organize shadows by their isomorphism type. We assume for the rest of the section that $q > 2$. Lemma 3.19 legitimates the following definitions:

DEFINITION 3.20. For all $r \in \mathbb{N}$, we choose a set of representatives for the collection of all isomorphism classes of group-shadows of elements in \mathfrak{h}_r and we denote it with $\mathfrak{Sh}(\mathfrak{h}_r)$ and call its members *isomorphism types* of shadows of level r . We choose a set of representatives for the collection of all group shadows of all \mathfrak{h}_t ($t \in \mathbb{N}$). We denote this set with

$$\mathfrak{Sh}(\mathfrak{h})$$

and call its elements isomorphism types of shadows. In what follows we shall indicate isomorphism types of shadows (of level r) with boldface roman capitals, e.g. \mathbf{S} . Let $\mathbf{S} \in \mathfrak{Sh}(\mathfrak{h}_r)$ and $\mathbf{T} \in \mathfrak{Sh}(\mathfrak{h}_{r+1})$.

DEFINITION 3.21. Let $r \in \mathbb{N}$ and $\mathbf{S} \in \mathfrak{Sh}(\mathfrak{h}_r)$. We define

$$d_{\mathbf{S}} = \dim_{\mathbb{F}_q} \text{As}(\mathbf{S}).$$

Notice that if $a \in \mathfrak{h}_r$ and $\text{Sh}_{G_r}(a) \cong \mathbf{S}$, then $d_{\mathbf{S}} = \dim_{\mathbb{F}_q} \text{Sh}_{\mathfrak{h}_r}(a)$ by Lemma 3.19. The number $d_{\mathbf{S}}$ is called the *dimension* of \mathbf{S} .

DEFINITION 3.22. Let $r \in \mathbb{N}$, $\mathbf{S} \in \mathfrak{Sh}(\mathfrak{h}_r)$ and $\mathbf{T} \in \mathfrak{Sh}(\mathfrak{h}_{r+1})$. We define

$$\Lambda(\mathbf{S}, \mathbf{T}) = |\{c \in \text{As}(\mathbf{S})^\sharp \mid \text{Stab}_{\mathbf{S}}(c) \cong \mathbf{T}\}|.$$

Let $a \in \mathfrak{h}_r$ with $\text{Sh}_{G_r}(a) \cong \mathbf{S}$. Assume that a admits a shadow-preserving lift and let $\mathbf{T} \in \mathfrak{Sh}(\mathfrak{h}_{r+1})$. From Lemma 3.19 it follows that

$$\Lambda(\mathbf{S}, \mathbf{T}) = |\{c \in \text{Sh}_{\mathfrak{h}_r}(a)^\sharp \mid \text{Stab}_{\mathbf{S}}(c) \cong \mathbf{T}\}|.$$

In view of this we may prove the following refined version of Theorem C.

COROLLARY 3.23. Let $\mathbf{S}, \mathbf{T} \in \mathfrak{Sh}(\mathfrak{h})$. Let $r \in \mathbb{N}$ and $a \in \mathfrak{h}_r$ with $\text{Sh}_{G_r}(a) \cong \mathbf{S}$. Assume further that $a \in \mathfrak{h}_r$ admits a shadow-preserving lift. Then the number of lifts of a with shadow isomorphic to \mathbf{T} is equal to

$$q^{d-d_{\mathbf{S}}} \Lambda(\mathbf{S}, \mathbf{T}).$$

REMARK 3.24. The proposition above has the important consequence that the number of lifts of an element of $a \in \mathfrak{h}_r$ with shadow isomorphic to \mathbf{T} only depends on (the isomorphism type of) $\text{Sh}_{G_r}(a)$ and on \mathbf{T} , not on the choice of a or on r .

4. APPLICATIONS TO REPRESENTATION ZETA FUNCTIONS

4.1. Potent and saturable pro- p groups. This section serves the purpose of introducing the tools we shall need to apply Theorems A and B to the computation of representation zeta functions of almost all of the principal congruence subgroups of $\text{SL}_3(\mathfrak{o})$. Assume that $G = \mathbf{G}(\mathfrak{o})$ is rigid (i.e. its number of continuous complex i -dimensional irreducible representations is finite for each $i \in \mathbb{N}$).

4.1.1. Kirillov orbit method. We say that $m \in \mathbb{N}$ is permissible for G when $G^m = \mathbf{G}^m(\mathfrak{o})$ is potent and saturable (c.f. [3, Section 2.1] for a definition of potent and saturable groups). [3, Proposition 2.3] ensures that there is $m_0 \in \mathbb{N}$ such that m is permissible for $m \geq m_0$. Fix a permissible $m \in \mathbb{N}$ and let $\mathfrak{g}^m = \text{L}(G^m)$.

First developed by Howe in [19] in the realm of compact p -adic analytic groups and applied to the study of representation zeta functions of FAb compact p -adic analytic groups by Jaikin-Zapirain in [21], the Kirillov orbit method is a powerful tool that completely describes the irreducible representations of a group in terms of co-adjoint orbits in an \mathbb{Z}_p -Lie lattice associated with the group. The version that we employ works with potent and saturable pro- p groups and it is due to Gonzalez-Sanchez (see [16] for a more exhaustive description).

We consider the Pontryagin dual of the compact abelian group $(\mathfrak{g}^m, +)$

$$\text{Irr}(\mathfrak{g}^m) = \widehat{\mathfrak{g}^m} = \text{Hom}_{\mathbb{Z}}^{\text{cont}}(\mathfrak{g}^m, \mathbb{C}^*),$$

i.e. the group $\text{Hom}_{\mathbb{Z}}^{\text{cont}}(\mathfrak{g}^m, \mathbb{C}^*) = \text{Hom}_{\mathbb{Z}}^{\text{cont}}(\mathfrak{g}^m, \mu_{p^\infty})$ of continuous complex characters of the additive group \mathfrak{g}^m , where $\mu_{p^\infty} \cong \mathbb{Q}_p/\mathbb{Z}_p$ is the group of complex roots of unity of order a power of p . With each $\omega \in \text{Irr}(\mathfrak{g}^m)$ we associate a biadditive bilinear form

$$\begin{aligned} b_\omega : \mathfrak{g}^m \times \mathfrak{g}^m &\longrightarrow \mu_{p^\infty} \\ (x, y) &\longmapsto \omega([x, y]). \end{aligned}$$

We define the radical of the bilinear form b_ω as

$$\text{Rad}(\omega) = \text{Rad}(b_\omega) = \{x \in \mathfrak{g}^m \mid \forall y \in \mathfrak{g}^m : b_\omega(x, y) = 1\}.$$

The Kirillov orbit method implies that there is a one to one correspondence between orbits for the G^m -co-adjoint action on $\widehat{\mathfrak{g}^m}$ and continuous complex irreducible representations of G^m . In particular

$$(4.1) \quad \zeta_{G^m}(s) = \sum_{\omega \in \text{Irr}(\mathfrak{g}^m)} |\mathfrak{g}^m : \text{Rad}(\omega)|^{-\frac{s+2}{2}}$$

(c.f. [16, Corollary 2.13] and [21, Theorem 5.2]).

4.1.2. Commutator matrix and Poincaré series. We give a short summary of some facts in [3, Section 2.2, Section 3.1]. Notice that by Proposition 2.6, we may assume that $\mathfrak{g}^m = \pi^m \text{Lie}(\mathbf{G})(\mathfrak{o})$, therefore let $\mathfrak{g} = \text{Lie}(\mathbf{G})(\mathfrak{o})$, so that $\mathfrak{g}^m = \pi^m \mathfrak{g}$. Let \mathfrak{k} be the field of fractions of \mathfrak{o} and set $\dim_{\mathfrak{k}}(\mathfrak{k} \otimes_{\mathfrak{o}} \mathfrak{g}) = d$. The following lemma explains how to conveniently sort irreducible representations of the Lie lattice \mathfrak{g} .

LEMMA 4.1 ([3, Lemma 2.4]). *The dual of an \mathfrak{o} -Lie lattice \mathfrak{g} can be written as a disjoint union:*

$$\widehat{\mathfrak{g}} = \bigcup_{r \in \mathbb{N}_0} \text{Irr}_r(\mathfrak{g}), \text{ where } \text{Irr}_r(\mathfrak{g}) \cong \text{Hom}_{\mathfrak{o}}(\mathfrak{g}, \mathfrak{o}/\mathfrak{p}^r)^*.$$

For $r \in \mathbb{N}_0$, an element of $\omega \in \text{Irr}_r(\mathfrak{g})$ is said to have level $\text{lev}(\omega) = r$. The sets $\text{Irr}_r(\mathfrak{g}^m)$ are G^m -invariant and therefore each irreducible representation of G^m corresponds to a unique co-adjoint orbit $\mathcal{C} \subseteq \text{Irr}_r(\mathfrak{g}^m)$ for some level $r \in \mathbb{N}_0$.

Thanks to this categorization of irreducible representations, it is possible to rephrase the problem of counting representations in a counting problem involving a matrix of linear forms with coefficients in \mathfrak{o} .

4.1.3. Commutator matrix. We choose an \mathfrak{o} -basis $\mathcal{B} = \{b_1, \dots, b_d\}$ for the \mathfrak{o} -Lie lattice \mathfrak{g} . For any $b_i, b_j \in \mathcal{B}$, there are $\lambda_{i,j}^1, \dots, \lambda_{i,j}^d \in \mathfrak{o}$ such that

$$[b_i, b_j] = \sum_{h=1}^d \lambda_{i,j}^h b_h.$$

The coefficients $\lambda_{i,j}^h$ for $i, j, h = 1, \dots, d$ are called the *structure constants* of \mathfrak{g} with respect to \mathcal{B} . By means of them we define the *commutator matrix* of \mathfrak{g} as

$$(4.2) \quad \mathcal{R}_{\mathcal{B}}(\mathbf{Y}) = \left(\sum_{h=1}^d \lambda_{i,j}^h Y_h \right)_{i,j} \in \text{Mat}_d(\mathfrak{o}[\mathbf{Y}])$$

with variables $\mathbf{Y} = (Y_1, \dots, Y_d)$.

NOTATION 4.2. Let $n_1, n_2 \in \mathbb{N}$ and

$$\mathcal{R} = (g_{ij})_{i,j=1,\dots,n_1} \in \text{Mat}_{n_1}(\mathfrak{o}[Y_1, \dots, Y_{n_2}]).$$

We write

$$\mathcal{R}^r = (\theta_r(g_{ij}))_{i,j=1,\dots,n_1}$$

for the reduction mod \mathfrak{p}^r of \mathcal{R} . When $r = 1$ we write $\overline{\mathcal{R}} = \mathcal{R}^1$.

We consider now $\mathbf{w} = (w_1, \dots, w_d) \in W(\mathfrak{o}) = (\mathfrak{o}^d)^*$; the matrix $\mathcal{R}_{\mathcal{B}}(\mathbf{w})$ is an antisymmetric $d \times d$ matrix. Therefore its elementary divisors can be arranged in $h = \lfloor d/2 \rfloor$ pairs $(\mathfrak{p}^{a_1}, \mathfrak{p}^{a_1}), \dots, (\mathfrak{p}^{a_h}, \mathfrak{p}^{a_h})$ for $0 \leq a_1 \leq \dots \leq a_h \in (\mathbb{N}_0 \cup \{\infty\})$ together with $\mathfrak{p}^\infty = \{0\}$ if d is odd. We define

$$\nu(\mathcal{R}_{\mathcal{B}}(\mathbf{w})) = (a_1, \dots, a_h).$$

For $r \in \mathbb{N}$, let

$$(4.3) \quad W_r(\mathfrak{o}) = (W(\mathfrak{o}) + (\mathfrak{p}^r)^{(d)})/(\mathfrak{p}^r)^{(d)} = ((\mathfrak{o}/\mathfrak{p}^r)^d)^*.$$

Let $\mathbf{w}_r = (\theta_r(w_1), \dots, \theta_r(w_d))$. The valuation of the matrix $\mathcal{R}_{\mathcal{B}}^r(\mathbf{w}_r)$ is defined as

$$\nu(\mathcal{R}_{\mathcal{B}}^r(\mathbf{w}_r)) = (\min\{a_i, r\})_{i=1,\dots,h} \in \{0, 1, \dots, r\}^h.$$

Recall that, in order to apply the Kirillov orbit method, we work with the congruence sublattices $\mathfrak{g}^m = \pi^m \mathfrak{g}$. We derive an \mathfrak{o} -basis for \mathfrak{g}^m from \mathcal{B} by multiplying all of its elements by π^m . In other words we define a coordinate system

$$\mathfrak{g}^m \longrightarrow \mathfrak{o}^d, \quad z = \sum_{i=1}^d z_i(\pi^m b_i) \longmapsto \mathbf{z} = (z_1, \dots, z_d).$$

DEFINITION 4.3. We define

$$\mathcal{B}^\sharp = \{b_1^\sharp, \dots, b_d^\sharp\} \subseteq \text{Hom}_{\mathfrak{o}}(\mathfrak{g}, \mathfrak{o})$$

by $b_i^\sharp(b_j) = \delta_{i,j}$ for all $i, j \in \{1, \dots, d\}$. It is a standard computation to see that \mathcal{B}^\sharp is an \mathfrak{o} -basis for $\mathfrak{g}^\sharp = \text{Hom}_{\mathfrak{o}}(\mathfrak{g}, \mathfrak{o})$. Therefore we call \mathcal{B}^\sharp the dual basis to \mathcal{B} .

We define a coordinate system on $\text{Hom}_{\mathfrak{o}}(\mathfrak{g}^m, \mathfrak{o})$ by shifting the dual basis \mathcal{B}^\sharp :

$$\text{Hom}_{\mathfrak{o}}(\mathfrak{g}^m, \mathfrak{o}) \longrightarrow \mathfrak{o}^d, \quad w = \sum_{i=1}^d w_i(\pi^{-m} b_i^\sharp) \longmapsto \mathbf{w} = (w_1, \dots, w_d).$$

Since \mathcal{B}^\sharp is the dual basis of \mathcal{B} , we have that $w(z) = \mathbf{w} \cdot \mathbf{z}$ for z and w as above.

DEFINITION 4.4. Let $r \in \mathbb{N}$. We say that $w \in \text{Hom}_{\mathfrak{o}}(\mathfrak{g}^m, \mathfrak{o})$ is a *representative* of $\omega \in \text{Irr}_r(\mathfrak{g}^m)$ when ω is the image of w in the natural surjection

$$\text{Hom}_{\mathfrak{o}}(\mathfrak{g}^m, \mathfrak{o})^* \rightarrow \text{Hom}_{\mathfrak{o}}(\mathfrak{g}^m, \mathfrak{o}/\mathfrak{p}^r)^* \cong \text{Irr}_r(\mathfrak{g}^m),$$

where $\text{Irr}_r(\mathfrak{g}^m)$ is defined as in Lemma 4.1. A representative w of $\omega \in \text{Irr}_r(\mathfrak{g}^m)$ can be used to compute $\text{Rad}(\omega)$ as the following explains.

DEFINITION 4.5. Let $m, r \in \mathbb{N}_0$. Consider $\omega \in \text{Irr}_r(\mathfrak{g}^m)$ and let $w \in \text{Hom}_{\mathfrak{o}}(\mathfrak{g}^m, \mathfrak{o})^*$ represent ω . We define

$$\begin{aligned} \text{Rad}(w) &= \{x \in \mathfrak{g}^m \mid \forall y \in \mathfrak{g}^m : w([x, y]) = 0\} \\ \text{Rad}_r(w) &= \{x \in \mathfrak{g}^m \mid \forall y \in \mathfrak{g}^m : w([x, y]) \equiv 0 \pmod{\mathfrak{p}^r}\}. \end{aligned}$$

If $\omega \in \text{Irr}_r(\mathfrak{g}^m)$ is represented by w , then $z \in \text{Rad}(\omega)$ if and only if $z \in \text{Rad}_r(w)$. Expressing this in coordinates we can highlight the link between the Kirillov orbit method and the commutator matrix.

LEMMA 4.6. *Let $\omega \in \text{Irr}_r(\mathfrak{g}^m)$ and let $w \in \text{Hom}_{\mathfrak{o}}(\mathfrak{g}^m, \mathfrak{o})^*$ be one of its representatives. Let \mathbf{w} be the coordinates of w in the \mathfrak{o} -basis \mathcal{B}^\sharp and let $r \in \mathbb{N}_0$. Then for every $z \in \mathfrak{g}^m$ with \mathcal{B} -coordinates $\mathbf{z} \in \mathfrak{o}^d$ we have*

$$\begin{aligned} z \in \text{Rad}(w) &\iff \mathbf{z} \cdot \mathcal{R}_{\mathcal{B}}(\mathbf{w}) = 0, \\ z \in \text{Rad}_r(w) &\iff \mathbf{z} \cdot \pi^m \mathcal{R}_{\mathcal{B}}(\mathbf{w}) \equiv 0 \pmod{\mathfrak{p}^r}. \end{aligned}$$

PROOF. The first double implication follows immediately from the definition of commutator-matrix, indeed for all $x, y \in \mathfrak{g}^m$ we have $w([x, y]) = \pi^m \mathbf{x} \mathcal{R}_{\mathcal{B}}(\mathbf{w}) \mathbf{y}^t$, where \mathbf{x} and \mathbf{y} are the coordinates of x and y in the basis $\pi^m \mathcal{B}$. The second double implication is [3, Lemma 3.3]. \square

4.1.4. *Poincaré series.* We briefly recall the definition of the Poincaré series associated with a matrix of linear forms and its relation with the representation zeta function of G^m for each permissible $m \in \mathbb{N}$ as expressed in [3, Section 3]. We borrow the notation from [32, Section 3.1].

Let $\mathcal{R} \in \text{Mat}_d(\mathfrak{o}[\mathbf{Y}])$ be an antisymmetric matrix of linear forms in f variables. Let $I = \{i_1, \dots, i_\ell\}_< \subseteq [h-1]_0$. We impose $i_0 = 0$ and $i_{\ell+1} = h$ and we write

$$\mu_j = i_{j+1} - i_j$$

with $j \in [\ell]_0$ (so $\mu_\ell = h - i_\ell$). For $\mathbf{r}_I = (r_1, \dots, r_\ell) \in \mathbb{N}^{|I|}$, we set $N = \sum_{j=1}^\ell r_j$ and. We define

$$\begin{aligned} N_{I, \mathbf{r}_I}^\circ(\mathcal{R}) = \{ \mathbf{w} \in W_N(\mathfrak{o}) \mid \nu(\mathcal{R}(\mathbf{w})) = & \underbrace{(0, \dots, 0)}_{\mu_\ell} \underbrace{(r_\ell, \dots, r_\ell)}_{\mu_{\ell-1}}, \\ & \underbrace{(r_\ell + r_{\ell-1}, \dots, r_\ell + r_{\ell-1})}_{\mu_{\ell-2}} \dots, \underbrace{(N, \dots, N)}_{\mu_0} \in \mathbb{N}_0^h \} \end{aligned}$$

and

$$\mathcal{P}_{\mathcal{R}}(s) = \sum_{\substack{I \subseteq [h-1]_0 \\ I = \{i_1, \dots, i_\ell\}_<}} \sum_{\mathbf{r}_I \in \mathbb{N}^{|I|}} |N_{I, \mathbf{r}_I}^\circ(\mathcal{R})| q^{-s \sum_{j=1}^\ell r_j (h - i_j)}.$$

Let $\mathcal{R} = \mathcal{R}_{\mathcal{B}}$ (in particular we have $f = d$). We set

$$(4.4) \quad N_{I, \mathbf{r}_I}^\circ(\mathfrak{g}) = |N_{I, \mathbf{r}_I}^\circ(\mathcal{R})|$$

This is clearly well defined as changing basis for \mathfrak{g} results in a linear invertible substitution of variables in the linear forms constituting the entries of \mathcal{R} . As a consequence we can define

$$(4.5) \quad \mathcal{P}_{\mathfrak{g}}(s) = \sum_{\substack{I \subseteq [h-1]_0 \\ I = \{i_1, \dots, i_\ell\}_<}} \sum_{\mathbf{r}_I \in \mathbb{N}^{|I|}} N_{I, \mathbf{r}_I}^\circ(\mathfrak{g}) q^{-s \sum_{j=1}^\ell r_j (h - i_j)}.$$

REMARK 4.7. Let $w \in N_{I, \mathbf{r}_I}^\circ(\mathcal{R})$, then the definition of $N_{I, \mathbf{r}_I}^\circ(\mathcal{R})$ entails that

$$\text{rk}_{\mathbb{F}_q} \overline{\mathcal{R}(w)} = h - i_\ell$$

where $\overline{\mathcal{R}(w)}$ is the reduction mod \mathfrak{p} of $\mathcal{R}(w)$.

The following illustrates the relation between the representation zeta function and the Poincaré series.

PROPOSITION 4.8 ([3, Proposition 3.1]). *For all m that are permissible for G*

$$\zeta_{G^m}(s) = q^{d \cdot m} \mathcal{P}_{\mathfrak{g}}(s + 2).$$

4.1.5. *Commutator matrices and rank-varieties.* We shall now explain the relation between the Lie shadow and the kernel of the commutator matrix. This will ultimately enable us to apply Theorem C to obtain the representation zeta function of the principal congruence subgroups of $\mathrm{SL}_3(\mathfrak{o})$.

Let $\mathfrak{k} = \mathrm{Frac}(\mathfrak{o})$. We fix an \mathfrak{o} -basis \mathcal{B} for \mathfrak{g} and we denote with \mathcal{R} the commutator matrix of \mathfrak{g} with respect to \mathcal{B} .

DEFINITION 4.9. For $2i \leq d$, let $P_i \subseteq \mathfrak{o}[\mathbf{Y}]$ be the ideal generated by the $2i \times 2i$ Pfaffians of \mathcal{R} . We write

$$V_{\mathcal{R}}^{2i} = \mathrm{Spec}(\mathfrak{o}[\mathbf{Y}]/P_i).$$

The *rank- $2i$ locus* $L_{\mathcal{R}}^{2i}$ of \mathcal{R} is the scheme-theoretic complement of $V_{\mathcal{R}}^{2(i-1)}$ as a closed subscheme of $V_{\mathcal{R}}^{2i}$.

LEMMA 4.10. Let \mathcal{B}' be another \mathfrak{o} -basis for \mathfrak{g} , and let S be the basis-change matrix from \mathcal{B} to \mathcal{B}' . Then, for all $\mathbf{v} \in \mathfrak{o}^d$,

$$S^t \mathcal{R}'(\mathbf{v}) S = \mathcal{R}(\mathbf{v}(S^{-1})^t),$$

where \mathcal{R}' the commutator matrix of \mathfrak{g} with respect to \mathcal{B}' .

PROOF. Let $\mathbf{v} = (v_1, \dots, v_d) \in \mathfrak{o}^d$. Let also $\mathcal{B}'^\# = \{b'_1, \dots, b'_d\}$ be the dual basis of \mathcal{B}' . The matrix $\mathcal{R}'(\mathbf{v})$ is the matrix of the bilinear form b_ω defined in Section 4.1.1 where $\omega = \sum_{i=1}^d v_i b'_i$. Since S is the basis change from \mathcal{B} to \mathcal{B}' , $\mathbf{v}(S^{-1})^t$ expresses the coordinates of ω with respect to \mathcal{B} . It follows that $\mathcal{R}(\mathbf{v}(S^{-1})^t)$ is the matrix of b_ω with respect to \mathcal{B} . Hence the equality with $S^t \mathcal{R}'(\mathbf{v}) S$. \square

DEFINITION 4.11. Let $r \in \mathbb{N}$. The choice of an \mathfrak{o} -basis for \mathfrak{g} determines coordinate systems

$$\begin{aligned} \iota : \mathfrak{g} &\rightarrow \mathfrak{o}^d \\ \iota_r : \mathfrak{g}_r &\rightarrow (\mathfrak{o}_r)^d. \end{aligned}$$

We write $\bar{\iota} = \iota_1$.

Fixed a coordinate system ι on \mathfrak{g} , we denote with η the dual of ι and with η_r the dual of ι_r . Recall that we denote with $\theta_r : \mathfrak{o} \rightarrow \mathfrak{o}_r$ the reduction modulo \mathfrak{p}^r and that, by an abuse of notation, θ_r also denotes the reduction modulo \mathfrak{p}^r on \mathfrak{g} ; we shall denote with the same symbol the reduction modulo \mathfrak{p}^r on $(\mathfrak{o})^d$ too.

NOTATION 4.12. We denote with β be the isomorphism from \mathfrak{g} to $\mathfrak{g}^\# = \mathrm{Hom}_{\mathfrak{o}}(\mathfrak{g}, \mathfrak{o})$ defined by the invariant non-degenerate symmetric form κ . Let, for $r \in \mathbb{N}$,

$$\beta_r : \mathfrak{g}_r \rightarrow \mathfrak{g}_r^\# = \mathrm{Hom}_{\mathfrak{o}}(\mathfrak{g}, \mathfrak{o}_r)$$

be the \mathfrak{o}_r -modules isomorphism induced by β . Let $\xi_r = \eta_r^{-1} \circ \beta_r$ for $r \in \mathbb{N}$ and $\xi = \eta^{-1} \circ \beta$.

REMARK 4.13. By Definition 4.11, the following diagrams commute

$$\begin{array}{ccc} \mathfrak{g} & \xrightarrow{\xi} & (\mathfrak{o})^d \\ \theta_r \downarrow & & \downarrow \theta_r \\ \mathfrak{g}_r & \xrightarrow{\xi_r} & (\mathfrak{o}_r)^d, \end{array}$$

for all $r \in \mathbb{N}$.

Let $\mathcal{L} = \mathrm{Lie}(\mathbf{G})(\mathbb{C})$. For $2k \leq d$, we denote the \mathfrak{o} -integral points on the loci of constant centralizer dimension with

$$X_{\mathcal{L}}^{d-2k}(\mathfrak{o}) = \{x \in \mathfrak{g} \mid \mathrm{rk}_{\mathfrak{o}} C_{\mathfrak{g}}(x) = d - 2k\},$$

and with $L_{\mathcal{R}}^{2k}(\mathfrak{o})$ the \mathfrak{o} -integral points of the rank-locus $L_{\mathcal{R}}^{2k}$.

LEMMA 4.14. *Let $x \in \mathfrak{g}_r$. Then, $\xi X_{\mathcal{L}}^{d-2k}(\mathfrak{o}) = L_{\mathcal{R}}^{2k}(\mathfrak{o})$ and*

$$\dim_{\mathbb{F}_q} \overline{\ker_{\mathfrak{o}_r} \mathcal{R}^r(\xi_r(x))} = \dim_{\mathbb{F}_q} \text{Sh}_{\mathfrak{g}_r}(x),$$

where $\overline{\ker_{\mathfrak{o}_r} \mathcal{R}^r(\xi_r(x))}$ is the reduction mod \mathfrak{p} of $\ker_{\mathfrak{o}_r} \mathcal{R}^r(\xi_r(x))$.

PROOF. We mimic the argument in [3, Section 5]. Let $x \in \mathfrak{g}$. Then

$$\begin{aligned} \text{Rad}(\kappa(x, \cdot)) &= \{y \in \mathfrak{g} \mid \forall z \in \mathfrak{g} : \kappa(x, [y, z]) = 0\} \\ &= \{y \in \mathfrak{g} \mid \forall z \in \mathfrak{g} : \kappa([x, y], z) = 0\} \\ &= \{y \in \mathfrak{g} \mid [x, y] = 0\} \\ &= C_{\mathfrak{g}}(x), \end{aligned}$$

where, in passing from the first to the second line, we used the associativity of the Killing form. Hence Lemma 4.6 implies that $\xi X_{\mathcal{L}}^{d-2k}(\mathfrak{o}) = L_{\mathcal{R}}^{2k}(\mathfrak{o})$. The compatibility of ξ with the reduction mod \mathfrak{p}^r (cf. Remark 4.13) and the observations before Lemma 4.6 suffice to conclude. \square

REMARK 4.15. In the same notation of Lemma 4.14, the dimension of the Lie shadow of x is equal to the number of maximal elementary divisors of $\mathcal{R}^r(\xi_r(x))$ because the latter is equal to

$$\dim_{\mathbb{F}_q} \overline{\ker_{\mathfrak{o}_r} \mathcal{R}^r(\xi_r(x))}.$$

4.2. The Poincaré series of $\mathfrak{sl}_3(\mathfrak{o})$. The Lie ring $\mathfrak{sl}_3(\mathfrak{o})$ is shadow-hereditary (cf. [4, Lemma 6.4]). In this case Section 3.6 gives a direct way of computing the Poincaré series. As a result we obtain the representation zeta function of $\text{SL}_3^m(\mathfrak{o})$ when $q > 2$ and $3 \nmid q$. Throughout the rest of this section $\mathbf{G} = \text{SL}_3$ (hence $d = 8$ and $h = 4$). The normalized Killing form described in [3, Section 6.1] is non-degenerate for $3 \nmid q$. We assume from now on that $3 \nmid q$ and, in order to apply Corollary 3.23, that $q > 2$. We denote with κ the non-degenerate form.

4.2.1. Poincaré series with shadows. First of all we rephrase the summation defining the Poincaré series so that it fits the language of shadows introduced in Section 3. We shall need some notation: let \mathbf{S} be an isomorphism type of shadows. Recall that in Definition 3.21 we defined $d_{\mathbf{S}} = \dim_{\mathbb{F}_q} \text{As}(\mathbf{S})$. For $\mathbf{S} \in \mathfrak{Sh}(\mathfrak{sl}_3(\mathfrak{o}))$ we define

$$\delta(\mathbf{S}) = \frac{1}{2}(d - d_{\mathbf{S}}) = h - \left\lfloor \frac{1}{2}d_{\mathbf{S}} \right\rfloor.$$

Notice that $\delta(\mathbf{S})$ is an integer. Indeed, by Lemma 4.14, $d - d_{\mathbf{S}}$ is the number of invertible elementary divisors of an antisymmetric matrix and therefore even.

DEFINITION 4.16. A *decreasing sequence of shadows* is a set of isomorphism types of shadows

$$\{\mathbf{S}_1, \dots, \mathbf{S}_{\ell}\}$$

such that for $0 < i < j \leq \ell$ we have $d_{\mathbf{S}_i} > d_{\mathbf{S}_j}$. The set of all decreasing sequences of shadows is denoted with \mathcal{D} .

DEFINITION 4.17. Let $\mathcal{I} = \{\mathbf{S}_1, \dots, \mathbf{S}_{\ell}\} \in \mathcal{D}$ and $\mathbf{r}_{\mathcal{I}} = (r_{\mathbf{S}_1}, \dots, r_{\mathbf{S}_{\ell}}) \in \mathbb{N}^{\mathcal{I}}$. Let $N = \sum_{\mathbf{S} \in \mathcal{I}} r_{\mathbf{S}}$ and $W_N(\mathfrak{o})$ be as in (4.3). We define

$$\begin{aligned} &\mathcal{N}_{\mathcal{I}, \mathbf{r}_{\mathcal{I}}}(\mathfrak{sl}_3(\mathfrak{o})) \\ &= \left\{ x \in W_N(\mathfrak{o}) \mid \forall \mathbf{S}_i \in \mathcal{I} \forall r \in \left(\sum_{j \leq i} r_{\mathbf{S}_j}, \sum_{j \leq i+1} r_{\mathbf{S}_j} \right) : \text{Sh}_{\text{SL}_3(\mathfrak{o}_t)}(\theta_r(x)) \cong \mathbf{S}_i \right\}. \end{aligned}$$

Definition 4.17 allows us to rewrite the Poincaré series of $\mathfrak{sl}_3(\mathfrak{o})$: for $I = \{i_1, \dots, i_\ell\}_< \subseteq [h-1]_0$, we define

$$\mathcal{D}_I = \{\{\mathbf{S}_1, \dots, \mathbf{S}_\ell\} \in \mathcal{D} \mid \delta(\mathbf{S}_j) = i_j \forall j \in \{1, \dots, \ell\}\}.$$

Now set $\mathbf{r}_{\mathcal{I}} = \mathbf{r}_I$ for all $\mathcal{I} \in \mathcal{D}_I$. It follows from the definition of $N_{I, \mathbf{r}_I}^\circ(\mathfrak{sl}_3(\mathfrak{o}))$ (see (4.4)), Lemma 4.14 and Remark 4.15 that

$$N_{I, \mathbf{r}_I}^\circ(\mathfrak{sl}_3(\mathfrak{o})) = \sum_{\mathcal{I} \in \mathcal{D}_I} |\mathcal{N}_{\mathcal{I}, \mathbf{r}_{\mathcal{I}}}(\mathfrak{sl}_3(\mathfrak{o}))|.$$

With (4.5), this implies

$$(4.6) \quad \mathcal{P}_{\mathfrak{sl}_3(\mathfrak{o})}(s) = \sum_{\mathcal{I} \in \mathcal{D}} \sum_{\mathbf{r}_{\mathcal{I}} \in \mathbb{N}^{\mathcal{I}}} |\mathcal{N}_{\mathcal{I}, \mathbf{r}_{\mathcal{I}}}(\mathfrak{sl}_3(\mathfrak{o}))| q^{-s \sum_{\mathbf{S} \in \mathcal{I}} r_{\mathbf{S}} \cdot \delta(\mathbf{S})}.$$

4.2.2. *A multiplicative formula for the Poincaré series.* We shall now use the results in Section 3.6 to give a multiplicative form for the Poincaré series of $\mathfrak{sl}_3(\mathfrak{o})$.

LEMMA 4.18. *Consider $\mathcal{I} = \{\mathbf{S}_1, \dots, \mathbf{S}_\ell\} \in \mathcal{D}$. Let $\mathbf{r}_{\mathcal{I}} = (r_{\mathbf{S}_1}, \dots, r_{\mathbf{S}_\ell}) \in \mathbb{N}^{\mathcal{I}}$. Let $\mathbf{S}_0 = \mathrm{SL}_3(\mathbb{F}_q)$ and $\mathcal{N}_{\mathcal{I}, \mathbf{r}_{\mathcal{I}}}(\mathfrak{sl}_3(\mathfrak{o}))$ be as in Definition 4.17. Then*

$$|\mathcal{N}_{\mathcal{I}, \mathbf{r}_{\mathcal{I}}}(\mathfrak{sl}_3(\mathfrak{o}))| = \prod_{\mathbf{S}_i \in \mathcal{I}} \left(\Lambda(\mathbf{S}_{i-1}, \mathbf{S}_i) \cdot q^{d-d_{\mathbf{S}_{i-1}}} \right) \cdot \prod_{\mathbf{S} \in \mathcal{I}} \left(\Lambda(\mathbf{S}, \mathbf{S}) \cdot q^{d-d_{\mathbf{S}}} \right)^{r_{\mathbf{S}}-1}.$$

PROOF. Let $a \in \mathfrak{sl}_3(\mathfrak{o}_r)$ with $\mathrm{Sh}_{\mathfrak{sl}_3(\mathfrak{o}_r)}(a) \cong \mathbf{S}$, we denote with $c_{\mathbf{S}, \mathbf{T}}$ the number of lifts of a to $\mathfrak{sl}_3(\mathfrak{o}_{r+1})$ whose shadow is isomorphic to \mathbf{T} . By Remark 3.24 $c_{\mathbf{S}, \mathbf{T}}$ is independent of the choice of a . By definition of $\mathcal{N}_{\mathcal{I}, \mathbf{r}_{\mathcal{I}}}(\mathfrak{sl}_3(\mathfrak{o}))$ (Definition 4.17) we have that

$$|\mathcal{N}_{\mathcal{I}, \mathbf{r}_{\mathcal{I}}}(\mathfrak{sl}_3(\mathfrak{o}))| = \Lambda(\mathrm{SL}_3(\mathbb{F}_q), \mathbf{S}_1) \cdot \prod_{\mathbf{S}_i \in \mathcal{I} \setminus \{\mathbf{S}_\ell\}} c_{\mathbf{S}_i, \mathbf{S}_{i+1}} \cdot \prod_{\mathbf{S} \in \mathcal{I}} c_{\mathbf{S}, \mathbf{S}}^{r_{\mathbf{S}}-1}.$$

Now it suffices to apply Corollary 3.23 to the equation above. \square

LEMMA 4.19. *Let $r \in \mathbb{N}$ and let $e \in \mathfrak{sl}_3(\mathfrak{o}_r)$. Let b be a shadow-preserving lift of e and $x = b + \pi^r x_c$ for $x_c \in \mathfrak{sl}_3(\mathfrak{o}_{r+1})$. Let $c = \gamma(\bar{\varphi}_r(\pi^r x_c + \pi \mathrm{im} \mathrm{ad}_b))$ where γ is as in (3.5) and $\bar{\varphi}_r$ as in Notation 3.5. Let also*

$$\mathrm{Stab}_{\mathrm{Sh}_{\mathfrak{sl}_3(\mathfrak{o}_r)}(e)}(c) = \{y \in \mathrm{Sh}_{\mathfrak{sl}_3(\mathfrak{o}_r)}(e) \mid c([y, z]) = 0 \forall z \in z \in \mathrm{Sh}_{\mathfrak{sl}_3(\mathfrak{o}_r)}(e)\}.$$

Then

$$\mathrm{Stab}_{\mathrm{Sh}_{\mathfrak{sl}_3(\mathfrak{o}_r)}(e)}(c) = \mathrm{Sh}_{\mathfrak{sl}_3(\mathfrak{o}_r)}(x).$$

PROOF. Let κ_1 be the \mathbb{F}_q -bilinear symmetric form on $\mathfrak{sl}_3(\mathbb{F}_q)$ induced by κ . By definition

$$c = \kappa_1(\bar{x}_c, -),$$

for $\bar{x}_c \equiv x_c \pmod{\mathfrak{p}}$. So $y \in \mathrm{Stab}_{\mathrm{Sh}_{\mathfrak{sl}_3(\mathfrak{o}_r)}(e)}(c)$ if and only if $\kappa_1(\bar{x}_c, [y, z]) = 0$ for all $z \in \mathrm{Sh}_{\mathfrak{sl}_3(\mathfrak{o}_r)}(e)$. If and only if

$$\kappa_1([\bar{x}_c, y], z) = 0 \text{ for all } z \in \mathrm{Sh}_{\mathfrak{sl}_3(\mathfrak{o}_r)}(e).$$

To see that this is equivalent to y being in $\mathrm{Sh}_{\mathfrak{sl}_3(\mathfrak{o}_{r+1})}(x)$, start by assuming that the latter holds. The shadow determines the Lie shadow and vice-versa (c.f. Lemma 3.19), and b is shadow-preserving, so $\mathrm{Sh}_{\mathfrak{sl}_3(\mathfrak{o}_r)}(e) = \mathrm{Sh}_{\mathfrak{sl}_3(\mathfrak{o}_{r+1})}(b)$. Moreover we may lift y to $\hat{y} \in \mathrm{C}_{\mathfrak{sl}_3(\mathfrak{o}_{r+1})}(x)$, obtaining

$$0 = [x, \hat{y}] = [b, \hat{y}] + [\pi^r x_c, \hat{y}].$$

It follows that $[\pi^r x_c, \hat{y}] \in \pi \mathrm{im} \mathrm{ad}_b$ and therefore $\kappa_1([\bar{x}_c, y], z) = 0$ for all $z \in \mathrm{Sh}_{\mathfrak{sl}_3(\mathfrak{o}_r)}(e)$. Indeed for all $w \in \mathfrak{sl}_3(\mathfrak{o}_{r+1})$ one has that $\kappa_1(\theta_{r+1,1}(w), y) = \gamma(\bar{\varphi}(\pi^r w +$

$\pi \operatorname{im} \operatorname{ad}_b)(z) = 0$ for all $z \in \operatorname{Sh}_{\mathfrak{sl}_3(\mathfrak{o}_r)}(e)$ if and only if $w \in \pi \operatorname{im} \operatorname{ad}_b$ because $\gamma \circ \bar{\varphi}$ is an isomorphism.

Conversely assume that $\kappa_1([\bar{x}_c, y], z) = 0$ for all $z \in \operatorname{Sh}_{\mathfrak{sl}_3(\mathfrak{o}_r)}(e)$. Choose a lift \hat{y} of y to $C_{\mathfrak{sl}_3(\mathfrak{o}_{r+1})}(b)$. We have that $\pi^r[x_c, \hat{y}] = \pi[b, w]$ for some $w \in \mathfrak{sl}_3(\mathfrak{o}_{r+1})$; hence $\hat{y} - \pi w$ centralizes x because

$$[x, \hat{y} - \pi w] = [b, \hat{y}] + \pi^r[x_c, \hat{y}] - \pi[b, w] = 0.$$

Since $y \equiv \hat{y} \equiv \hat{y} - \pi w \pmod{\mathfrak{p}}$, y is in the Lie shadow of x . \square

REMARK 4.20. Let $\mathbf{S} \in \mathfrak{Sh}(\mathfrak{sl}_3(\mathfrak{o}))$ and $\mathfrak{s} = \operatorname{As}(\mathbf{S})$. Let $\mathcal{B}_{\mathfrak{s}}$ be an \mathfrak{o} -basis for \mathfrak{s} and let $\mathcal{R}_{\mathfrak{s}}$ be the commutator matrix of \mathfrak{s} with respect to $\mathcal{B}_{\mathfrak{s}}$. Consider the fixed points

$$\operatorname{Triv}_{\mathbf{S}}(\mathfrak{s}^{\#}) = \{\omega \in \mathfrak{s}^{\#} \mid g \cdot \omega = \omega \forall g \in \mathbf{S}\} \subseteq \mathfrak{s}^{\#}$$

for the action of \mathbf{S} on $\mathfrak{s}^{\#}$. Corollary 3.23 says that

$$q^{d-\operatorname{ds}} |\operatorname{Triv}_{\mathbf{S}}(\mathfrak{s}^{\#})|$$

is the number of shadow-preserving lifts of an element with shadow isomorphic to \mathbf{S} . By Lemma 3.19, a lift of an element at level r preserves the shadows if and only if it preserves the Lie shadow, therefore, by Lemma 4.19, $\operatorname{Triv}_{\mathbf{S}}(\mathfrak{s}^{\#})$ is the set of elements for which $\mathcal{R}_{\mathfrak{s}}$ has rank 0, and therefore it is an \mathbb{F}_q -vector space of dimension $z_{\mathbf{S}} \in \mathbb{N}_0$, say. This implies

$$\Lambda(\mathbf{S}, \mathbf{S}) = |\operatorname{Triv}_{\mathbf{S}}(\mathfrak{s}^{\#})| = q^{z_{\mathbf{S}}}.$$

DEFINITION 4.21. Let \mathcal{I} and $\mathbf{r}_{\mathcal{I}}$ be as in Lemma 4.18. We define

$$f_{\mathcal{I}}(q) = q^{-(d-\operatorname{ds}_{\ell}) - \sum_{\mathbf{S} \in \mathcal{I}} z_{\mathbf{S}}} \cdot \prod_{\mathbf{S}_i \in \mathcal{I}} \Lambda(\mathbf{S}_{i-1}, \mathbf{S}_i).$$

Remark 4.20 allows us to restate Lemma 4.18 as follows.

LEMMA 4.22. Let \mathcal{I} and $\mathbf{r}_{\mathcal{I}}$ be as in Lemma 4.18. Then

$$|\mathcal{N}_{\mathcal{I}, \mathbf{r}_{\mathcal{I}}}(\mathfrak{sl}_3(\mathfrak{o}))| = f_{\mathcal{I}}(q) \cdot \prod_{\mathbf{S} \in \mathcal{I}} (q^{d-\operatorname{ds}+z_{\mathbf{S}}})^{r_{\mathbf{S}}}.$$

PROOF. According to Remark 4.20 we may write the equality of Lemma 4.18 as

$$|\mathcal{N}_{\mathcal{I}, \mathbf{r}_{\mathcal{I}}}(\mathfrak{sl}_3(\mathfrak{o}))| = \prod_{\mathbf{S}_i \in \mathcal{I}} \Lambda(\mathbf{S}_{i-1}, \mathbf{S}_i) \cdot q^{d-\operatorname{ds}_{i-1}} \cdot \prod_{\mathbf{S} \in \mathcal{I}} (q^{d-\operatorname{ds}+z_{\mathbf{S}}})^{r_{\mathbf{S}}-1}.$$

It remains to compute the telescopic sum $\sum_{\mathbf{S}_i \in \mathcal{I}} (d_{\mathbf{S}_i} - d_{\mathbf{S}_{i-1}}) = d_{\mathbf{S}_{\ell}} - d_{\mathbf{S}_0} = -(d - d_{\mathbf{S}_{\ell}})$. \square

We define

$$\mathbf{gp}(X) = \frac{X}{1-X}.$$

Lemma 4.22 and (4.6) imply the following:

$$(4.7) \quad \mathcal{P}_{\mathfrak{sl}_3(\mathfrak{o})}(s) = \sum_{\mathcal{I} \in \mathcal{D}} f_{\mathcal{I}}(q) \cdot \prod_{\mathbf{S} \in \mathcal{I}} \mathbf{gp}\left(q^{d-\operatorname{ds}+z_{\mathbf{S}}-s \cdot \delta(\mathbf{S})}\right).$$

4.3. The representation zeta function of $\operatorname{SL}_3^m(\mathfrak{o})$. Let $r \in \mathbb{N}$ and $a \in \mathfrak{sl}_3(\mathfrak{o}_r)$. We say that a is *regular* if $\dim_{\mathbb{F}_q} \operatorname{Sh}_{\mathfrak{sl}_3(\mathfrak{o}_r)}(a) = 2$ and that a is *subregular* if $\dim_{\mathbb{F}_q} \operatorname{Sh}_{\mathfrak{sl}_3(\mathfrak{o}_r)}(a) = 4$.

Consider a regular element $a \in \mathfrak{sl}_3(\mathfrak{o}_r)$ on level $r \in \mathbb{N}$. Its centralizer is abelian, so the action of $\operatorname{Sh}_{\operatorname{SL}_3(\mathfrak{o}_r)}(a)$ on $\operatorname{Sh}_{\mathfrak{sl}_3(\mathfrak{o}_r)}(a)^{\#}$ is trivial. For this reason we do not need to

distinguish regular elements according to their shadow and, for all $\mathbf{S} \in \mathfrak{Sh}(\mathfrak{sl}_3(\mathfrak{o}_r))$, we define

$$(4.8) \quad \Lambda(\mathbf{S}, \mathbf{R}) = \sum_{\substack{\mathbf{T} \in \mathfrak{Sh}(\mathfrak{sl}_3(\mathfrak{o}_{r+1})) \\ d_{\mathbf{T}}=2}} \Lambda(\mathbf{S}, \mathbf{T}).$$

Moreover, the set defined in Definition 4.17 does not include 0 and no other element of $\mathfrak{sl}_3(\mathfrak{o}_r)$ can have shadow equal to that of 0. It follows that we may exclude decreasing sequences starting with $\mathrm{SL}_3(\mathbb{F}_q)$ from those that we need in order to compute (4.7).

We start by considering the situation at level $r = 1$. That is to say, we look at orbits for the action of $\mathrm{SL}_3(\mathbb{F}_q)$ on $\mathfrak{sl}_3(\mathbb{F}_q)$. An analysis of the Frobenius rational forms in $\mathfrak{sl}_3(\mathbb{F}_q)$ reveals that the possible minimal polynomials of a subregular element are

$$m_\alpha = (X - \alpha)(X - 2\alpha),$$

where $\alpha \in \mathbb{F}_q$. In what follows we operate a case distinction depending on whether α is zero or not.

4.3.1. Subregular semisimple elements. Let $a \in \mathfrak{sl}_3(\mathbb{F}_q)$ have minimal polynomial

$$m_\alpha = (X - \alpha)(X - 2\alpha)$$

for $\alpha \in \mathbb{F}_q^\times$. Since the factors of m_α are linear and distinct, a is semisimple and diagonalizable, we observe that $\mathrm{Sh}_{\mathrm{SL}_3(\mathbb{F}_q)}(a) = \mathrm{C}_{\mathrm{SL}_3(\mathbb{F}_q)}(a) \cong \mathrm{GL}_2(\mathbb{F}_q)$. Let \mathbf{L} be the isomorphism type of the shadow of these elements. The orbit of a has cardinality

$$\frac{|\mathrm{SL}_3(\mathbb{F}_q)|}{|\mathrm{GL}_2(\mathbb{F}_q)|} = q^2(q^2 + q + 1).$$

Semisimple subregular elements form as many orbits as the possible different minimal polynomials m_α with $\alpha \neq 0$, i.e. $q - 1$. Therefore there are

$$(4.9) \quad \Lambda(\mathrm{SL}_3(\mathbb{F}_q), \mathbf{L}) = q^5 - q^2$$

subregular semisimple elements in total.

Moreover, the $\mathrm{Sh}_{\mathrm{SL}_3(\mathbb{F}_q)}(a)$ -action on $\mathrm{Sh}_{\mathfrak{sl}_3(\mathbb{F}_q)}(a)^\sharp$ is the adjoint action of $\mathrm{GL}_2(\mathbb{F}_q)$ on $\mathfrak{gl}_2(\mathbb{F}_q)$ and as a consequence

$$(4.10) \quad \begin{aligned} d_{\mathbf{L}} &= 4, \quad z_{\mathbf{L}} = 1 \\ \Lambda(\mathbf{L}, \mathbf{R}) &= q \cdot (q^3 - 1). \end{aligned}$$

4.3.2. Subregular nilpotent elements. All subregular elements that are not semisimple have minimal polynomial X^2 i.e. they are nilpotent. Let $a \in \mathfrak{sl}_3(\mathbb{F}_q)$ be such an element, and let

$$\mathbf{J} = \left\{ M = \begin{pmatrix} m_{11} & m_{12} & m_{13} \\ 0 & m_{11} & 0 \\ 0 & m_{32} & m_{33} \end{pmatrix} \middle| M \in \mathrm{SL}_3(\mathbb{F}_q) \right\}.$$

Then $\mathrm{Sh}_{\mathrm{SL}_3(\mathbb{F}_q)}(a) \cong \mathbf{J}$. We choose a basis for $\mathrm{As}(\mathbf{J})$:

$$e_0 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad e_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad e_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

TABLE 4.1. Lifting rules for $\mathrm{SL}_3^m(\mathfrak{o})$. **R** stands for any regular isomorphism type of shadows

S	$d_{\mathbf{S}}$	$z_{\mathbf{S}}$	$\delta(\mathbf{S})$	T	$\Lambda(\mathbf{S}, \mathbf{T})$
$\mathrm{SL}_3(\mathbb{F}_q)$	8	0	0	L	$(q^5 - q^2)$
				J	$(q^4 + q^3 - q - 1)$
				R	$q \cdot (q - 1) \cdot (q^6 + q^5 + q^4 - q^2 - 2q - 1)$
L	4	1	2	R	$q \cdot (q^3 - 1)$
J	4	1	2	R	$q \cdot (q^3 - 1)$
R	2	2	3	n.a.	n.a.

The basis $\mathcal{B} = \{e_0, \dots, e_3\}$ allows us to compute the commutator matrix

$$\mathcal{R}_{\mathcal{B}}(X_0, \dots, X_3) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 3X_2 & -3X_3 \\ 0 & -3X_2 & 0 & X_0 \\ 0 & 3X_3 & -X_0 & 0 \end{pmatrix}.$$

Let $f = 2$ or $f = 4$. Lemma 4.19 implies that the number elements in $c \in \mathrm{Sh}_{\mathfrak{sl}_3(\mathfrak{o}_r)}(a)^{\sharp}$ such that their **J**-stabilizer is isomorphic to **S** with $d_{\mathbf{S}} = f$ is

$$|\{\mathbf{x} \in \mathbb{F}_q^4 \mid \dim_{\mathbb{F}_q} \ker \mathcal{R}_{\mathcal{B}}(\mathbf{x}) = f\}|.$$

So (as we assumend $3 \nmid q$) there are q elements of $\mathrm{As}(\mathbf{J})^{\sharp}$ on which **J** acts trivially and $q^4 - q$ whose **J**-stabilizer is isomorphic to **S** with $d_{\mathbf{S}} = 4$. This gives us

$$(4.11) \quad \begin{aligned} d_{\mathbf{J}} &= 4, \quad z_{\mathbf{J}} = 1 \\ \Lambda(\mathbf{J}, \mathbf{R}) &= q \cdot (q^3 - 1). \end{aligned}$$

The centralizer of a subregular nilpotent element has cardinality $(q-1)q^3$, therefore

$$(4.12) \quad \Lambda(\mathrm{SL}_3(\mathbb{F}_q), \mathbf{J}) = q^4 + q^3 - q - 1.$$

Having considered all possible minimal polynomial of a non-zero element in $\mathfrak{sl}_3(\mathbb{F}_q)$ we conclude that except for $0 \in \mathfrak{sl}_3(\mathfrak{o}_r)$, whose shadow is $\mathrm{SL}_3(\mathbb{F}_q)$, elements of $\mathfrak{sl}_3(\mathfrak{o}_r)$ are either regular or subregular. In principle we would still need to complete the investigation for shadows appearing only at higher levels; however, since a lift of a subregular element is either regular or preserves the shadow, there cannot be other shadows of non-regular elements. It follows that the number of regular elements at level 1 is

$$(4.13) \quad \begin{aligned} \Lambda(\mathrm{SL}_3(\mathbb{F}_q), \mathbf{R}) &= q^8 - 1 - \Lambda(\mathrm{SL}_3(\mathbb{F}_q), \mathbf{J}) - \Lambda(\mathrm{SL}_3(\mathbb{F}_q), \mathbf{L}) \\ &= q \cdot (q - 1) \cdot (q^6 + q^5 + q^4 - q^2 - 2q - 1). \end{aligned}$$

Table 4.1 gives an overview of the results in equations (4.9) to (4.13) (see also [4, Table 2.2]). Recall that we excluded decreasing sequences starting with $\mathrm{SL}_3(\mathbb{F}_q)$ and therefore we do not need to consider lifts of 0. Again, as lifts of a subregular element are either regular or preserve the shadow, this table also describes the situation at all levels.

4.4. Representation zeta function. We can now compute the right-hand side of (4.7). We shall then be able to determine the Poincaré series of $\mathfrak{sl}_3(\mathfrak{o})$ when $q > 2$ and $3 \nmid q$.

First of all we work out the possible non-empty decreasing sequences of shadows for $\mathfrak{sl}_3(\mathfrak{o}) \setminus \{0\}$: these are $\{\mathbf{L}\}$, $\{\mathbf{J}\}$ and all $\{\mathbf{S}\}$, $\{\mathbf{L}, \mathbf{S}\}$ and $\{\mathbf{J}, \mathbf{S}\}$ where \mathbf{S} is a regular isomorphism type of shadow. For each decreasing sequence \mathcal{I} we shall now compute the product of geometric series associated with it and $f_{\mathcal{I}}(q)$. To do this it is convenient to make a distinction based on whether a decreasing sequence contains a 4-dimensional shadow or not. We keep the convention of not distinguishing among isomorphism types of regular shadows and, for all $\mathbf{S} \in \mathfrak{Sh}(\mathfrak{sl}_3(\mathfrak{o}))$, we define

$$\begin{aligned} f_{\{\mathbf{R}\}}(q) &= \sum_{\substack{\mathbf{T} \in \mathfrak{Sh}(\mathfrak{sl}_3(\mathfrak{o})) \\ d_{\mathbf{T}}=2}} f_{\{\mathbf{T}\}}(q) \\ f_{\{\mathbf{S}, \mathbf{R}\}}(q) &= \sum_{\substack{\mathbf{T} \in \mathfrak{Sh}(\mathfrak{sl}_3(\mathfrak{o})) \\ d_{\mathbf{T}}=2}} f_{\{\mathbf{S}, \mathbf{T}\}}(q). \end{aligned}$$

4.4.1. Decreasing sequences containing a subregular shadow. We collect all the summands corresponding to decreasing sequences that feature a 4-dimensional shadow. Let

$$\mathcal{D}_{sub} = \{ \{\mathbf{L}\}, \{\mathbf{J}\}, \{\mathbf{L}, \mathbf{T}\}, \{\mathbf{J}, \mathbf{T}\} \}_{\substack{\mathbf{T} \in \mathfrak{Sh}(\mathfrak{sl}_3(\mathfrak{o})) \\ d_{\mathbf{T}}=2}}$$

be the set containing all of these decreasing sequences. With the help of Table 4.1, a quick computation yields

$$\begin{aligned} f_{\{\mathbf{L}\}}(q) &= q^{-5} \Lambda(\mathrm{SL}_3(\mathbb{F}_q), \mathbf{L}) = q^{-5}(q^5 - q^2) \\ f_{\{\mathbf{J}\}}(q) &= q^{-5} \Lambda(\mathrm{SL}_3(\mathbb{F}_q), \mathbf{J}) = q^{-5}(q^4 + q^3 - q - 1) \\ f_{\{\mathbf{L}, \mathbf{R}\}}(q) &= q^{-9} \Lambda(\mathrm{SL}_3(\mathbb{F}_q), \mathbf{L}) \Lambda(\mathbf{L}, \mathbf{R}) = q^{-9}(q^9 - 2q^6 + q^3) \\ f_{\{\mathbf{J}, \mathbf{R}\}}(q) &= q^{-9} \Lambda(\mathrm{SL}_3(\mathbb{F}_q), \mathbf{J}) \Lambda(\mathbf{J}, \mathbf{R}) = q^{-9}(q^8 + q^7 - 2q^5 - 2q^4 + q^2 + q). \end{aligned}$$

We compute the following part of the summation in (4.7):

$$\begin{aligned} (4.14) \quad \mathcal{P}_{sub}(s) &= (f_{\{\mathbf{L}\}}(q) + f_{\{\mathbf{J}\}}(q)) \cdot \frac{q^{5-2s}}{1 - q^{5-2s}} \\ &\quad + (f_{\{\mathbf{L}, \mathbf{R}\}}(q) + f_{\{\mathbf{J}, \mathbf{R}\}}(q)) \cdot \frac{q^{13-5s}}{(1 - q^{8-3s})(1 - q^{5-2s})}. \end{aligned}$$

4.4.2. The regular shadow. The last non-empty decreasing sequences remaining are the ones containing only one regular shadow. By reading Table 4.1 we compute the summand in (4.7):

$$\begin{aligned} (4.15) \quad \mathcal{P}_{reg}(s) &= f_{\{\mathbf{R}\}}(q) \frac{q^{8-3s}}{1 - q^{8-3s}} = q^{-8} \Lambda(\mathrm{SL}_3(\mathbb{F}_q), \mathbf{R})(q) \frac{q^{8-3s}}{1 - q^{8-3s}} \\ &= q^{-8}(q^8 - q^5 - q^4 - q^3 + q^2 + q) \frac{q^{8-3s}}{1 - q^{8-3s}}. \end{aligned}$$

The empty shadow sequence gives rise to the summand 1, hence by (4.7)

$$\mathcal{P}_{\mathfrak{sl}_3(\mathfrak{o})}(s) = 1 + \mathcal{P}_{sub}(s) + \mathcal{P}_{reg}(s).$$

Operating the substitution in Proposition 4.8 we deduce the following special case of [3, Theorem E].

THEOREM D. *Let \mathfrak{o} be a compact discrete valuation ring of characteristic 0 whose residue field has cardinality $q > 2$ and characteristic $p \neq 3$. Then for all permissible m ,*

$$\zeta_{\mathrm{SL}_3^m(\mathfrak{o})}(s) = q^{8m} \frac{1 + u(q)q^{-3-2s} + u(q^{-1})q^{-2-3s} + q^{-5-5s}}{(1 - q^{1-2s})(1 - q^{2-3s})}$$

where $u(X) = X^3 + X^2 - X - 1 - X^{-1}$.

REFERENCES

- [1] H. Appelgate and H. Onishi. The similarity problem for 3×3 integer matrices. *Linear Algebra Appl.*, 42:159–174, 1982.
- [2] H. Appelgate and H. Onishi. Similarity problem over $\mathrm{SL}(n, \mathbf{Z}_p)$. *Proc. Amer. Math. Soc.*, 87(2):233–238, 1983.
- [3] N. Avni, B. Klopsch, U. Onn, and C. Voll. Representation zeta functions of compact p -adic analytic groups and arithmetic groups. *Duke Math. J.*, 162(1):111–197, 2013.
- [4] N. Avni, B. Klopsch, U. Onn, and C. Voll. Similarity classes of integral p -adic matrices and representation zeta functions of groups of type A_2 . *Proc. Lond. Math. Soc. (3)*, 112(2):267–350, 2016.
- [5] N. Avni, U. Onn, A. Prasad, and L. Vaserstein. Similarity classes of 3×3 matrices over a local principal ideal ring. *Comm. Algebra*, 37(8):2601–2615, 2009.
- [6] M. N. Berman, J. Derakhshan, U. Onn, and P. Paaajanen. Uniform cell decomposition with applications to Chevalley groups. *J. Lond. Math. Soc. (2)*, 87(2):586–606, 2013.
- [7] B. Conrad, O. Gabber, and G. Prasad. *Pseudo-reductive groups*, volume 26 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, second edition, 2015.
- [8] R. W. Davis. Certain matrix equations over rings of integers. *Duke Math. J.*, 35(1):49–59, 03 1968.
- [9] M. Demazure and P. Gabriel. *Introduction to algebraic geometry and algebraic groups*, volume 39 of *North-Holland Mathematics Studies*. North-Holland Publishing Co., Amsterdam-New York, 1980. Translated from the French by J. Bell.
- [10] J. Denef and L. van den Dries. p -adic and real subanalytic sets. *Ann. of Math. (2)*, 128(1):79–138, 1988.
- [11] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal. *Analytic pro- p groups*, volume 61 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1999.
- [12] J. A. Drozd. Tame and wild matrix problems. In *Representation theory, II (Proc. Second Internat. Conf., Carleton Univ., Ottawa, Ont., 1979)*, volume 832 of *Lecture Notes in Math.*, pages 242–258. Springer, Berlin-New York, 1980.
- [13] M. P. F. du Sautoy. Counting conjugacy classes. *Bull. London Math. Soc.*, 37(1):37–44, 2005.
- [14] D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.
- [15] J. González-Sánchez. On p -saturable groups. *J. Algebra*, 315(2):809–823, 2007.
- [16] J. González-Sánchez. Kirillov’s orbit method for p -groups and pro- p groups. *Comm. Algebra*, 37(12):4476–4488, 2009.
- [17] F. J. Grunewald. Solution of the conjugacy problem in certain arithmetic groups. In *Word problems, II (Conf. on Decision Problems in Algebra, Oxford, 1976)*, volume 95 of *Stud. Logic Foundations Math.*, pages 101–139. North-Holland, Amsterdam-New York, 1980.
- [18] F. J. Grunewald and D. Segal. The solubility of certain decision problems in arithmetic and algebra. *Bull. Amer. Math. Soc. (N.S.)*, 1(6):915–918, 1979.
- [19] R. E. Howe. Kirillov theory for compact p -adic groups. *Pacific J. Math.*, 73(2):365–381, 1977.
- [20] N. Jacobson. *Lie algebras*. Dover Publications, Inc., New York, 1979. Republication of the 1962 original.
- [21] A. Jaikin-Zapirain. Zeta function of representations of compact p -adic analytic groups. *J. Amer. Math. Soc.*, 19(1):91–118 (electronic), 2006.
- [22] S. Jambor and W. Plesken. Normal forms for matrices over uniserial rings of length two. *J. Algebra*, 358:250–256, 2012.
- [23] J. C. Jantzen. *Representations of algebraic groups*, volume 107 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, second edition, 2003.
- [24] B. Klopsch, N. Nikolov, and C. Voll. *Lectures on profinite topics in group theory*, volume 77 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 2011. Lectures from the course on Asymptotic Methods in Infinite Group Theory held in Oxford, September 2007, Edited by Dan Segal.

- [25] S. V. Nagornyĭ. Complex representations of the general linear group of degree three modulo a power of a prime. *Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)*, 75:143–150, 197–198, 1978. Rings and linear groups.
- [26] A. A. Nechaev. Similarity of matrices over a commutative local Artinian ring. *Trudy Sem. Petrovsk.*, (9):81–101, 1983.
- [27] J. Pas. Uniform p -adic cell decomposition and local zeta functions. *J. Reine Angew. Math.*, 399:137–172, 1989.
- [28] A. Pizarro. Similarity classes of 3×3 matrices over a discrete valuation ring. *Linear Algebra Appl.*, 54:29–51, 1983.
- [29] J. Pomfret. Similarity of matrices over finite rings. *Proc. Amer. Math. Soc.*, 37:421–422, 1973.
- [30] A. Prasad, P. Singla, and S. Spallone. Similarity of matrices over local rings of length two. *Indiana Univ. Math. J.*, 64(2):471–514, 2015.
- [31] P. Singla. On representations of general linear groups over principal ideal local rings of length two. *J. Algebra*, 324(9):2543–2563, 2010.
- [32] A. Stasinski and C. Voll. Representation zeta functions of nilpotent groups and generating functions for Weyl groups of type B . *Amer. J. Math.*, 136(2):501–550, 2014.
- [33] D. A. Suprunenko. On the conjugacy of matrices over a ring of residues. *Dokl. Akad. Nauk BSSR*, 8:693–695, 1964.
- [34] M. Zordan. *Representation zeta functions of special linear groups*. PhD thesis, Universität Bielefeld, <https://pub.uni-bielefeld.de/publication/2902722>, 2016.

FAKULTÄT FÜR MATHEMATIK, UNIVERSITÄT BIELEFELD, D-33501 BIELEFELD, GERMANY

E-mail address: `michele.zordan@math.uni-bielefeld.de`

Current address: Via San Pietro 9, 36016 Thiene (VI), Italy